

## Evaluation Scoring

### **Notes to Evaluators:**

Please provide detailed comments to assist in the consensus and debrief process.

**Suggested scoring valuation:** Please notice many of these points are not on a 1 to 5 scale and must be adjusted accordingly.

### **Remember to be consistent with scoring methodology**

#### **Example use only**

0	Did not provide an answer	Firm Experience	Staffing/Resumes	Sample
1	Incoherent, communicates a lack of understanding and/or capability	7	5	3
2	Marginal, communicates a weak knowledge, understanding, and/or capability	14	10	6
3	Average, communicates an average knowledge, understanding, and/or capability	21	15	9
4	Good, communicates that they are good at what they do and have a good understanding	28	20	12
5	Excellent, communicates that they are not just good, but provide value added services and capabilities that may exceed expectations	35	30	15

#### **Quotation Section (10%) Cost Proposal Score will be calculated by the contract manager.**

The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. This means that the overall score for the cost proposal will account for the robustness of the proposer's qualifications as well as their proposed price. We will include both the blended hourly rate and the price quote in scoring the cost proposal. The cost proposal will be worth up to 10 percent of the total possible points – see the table on page 26 of the RFQQ.

#### **Qualifications Section (65%)**

##### **Firm Experience (35%)**

The Qualifications Section of the proposal must contain information that will demonstrate to the evaluation committee the Firm/Staff understanding of the types of services proposed, the ability to accomplish them, and the ability to meet tight timeframes. Firm experience will be scored based on the capacity and experience of the firm to perform work similar to the tasks described in this RFQQ.

##### **Staff Experience/Resumes (30%)**

Staffing will be scored on how the proposer staffs the project to perform work similar to the tasks described in this RFQQ, including the number of staff and the mix or make of the team and their various levels of experience. see page 23 of the RFQQ for details. The proposer must provide a resume for key staff and include information on the individual's specific skills, experience, certifications, significant accomplishments and responsibilities assumed on other similar projects related to the services proposed.

#### **Sample Reports (15%)**

This sample report will be scored based on how well its components respond to items listed under item "e." under "Report Results" on page 4 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.

#### **Executive Order 18-03 & WA Small Business/Veteran Owned Business(10%) will be calculated by the contract manager.**

This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver.

Vendor Name	Score
Vendor: Accenture	62
Vendor: Affinity IT	44
Vendor: Berry Dunn	38
Vendor: BPM	48
Vendor: CAI	40
Vendor: Deloitte	50
Vendor: Digitech	58
Vendor: EideBailly	45
Vendor: Emagined	74
Vendor: ERM	66
Vendor: GSG	69
Vendor: Guidepost	40
Vendor: Inspira	69
Vendor: KPMG	55
Vendor: Lumen	59
Vendor: Online	65
Vendor: Peraton	73
Vendor: Plante Moran	48
Vendor: RSI	48
Vendor: SAC	52
Vendor: Shorebreak	71
Vendor: Soteria	69
Vendor: Spirent	70
Vendor: Summit	70
Vendor: System Soft	47
Vendor: Tevora	53
Vendor: WWT	38

K689 - Security Assessment Services			
Vendor: Accenture			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit. Michelle and Greg as leads over the penetration testing lead (no penetration test experience), and one full penetration test lead; One OT SME part time, one penetration tester full time and one firewall SME part time - so only two full time penetration testers which seems low for this large scope - two full time testers, two part time and two overhead managers with no penetration testing experience, noting it will take them 7 weeks
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	30.0	Firm experience with <u>state and local government</u> (State of Washington such as Department of Enterprise Services, Department of Social and Health Services, Liquor and Cannabis Board, and Department of Corrections just to name a few, as well as the City of Seattle, King County, and other public sector clients). <u>Testing methodology</u> clear and Discovery includes 20% automated and 80% manual techniques include misconfigurations, authentication missing patches and asset prioritization. Sensitive evidence collection. <u>Experience:</u> infrastructure (servers, workstations, network hardware, peripheral devices, eg), web and mobile applications, API, wireless, cloud infrastructure, and source code reviews. <u>Missing Thick client, mainframe, SCADA, includes API</u> Project <u>Representative Projects</u> <u>1: Penetration Testing Assessment</u> , North Carolina community College which included an Infrastructure Pen Test, Wireless Pen Test, Application Pen Test, source code review of custom code, and a vulnerability assessment on internal and cloud infrastructures, Improved AWS Security for future releases- this is good. <u>2. Project Ivy league University</u> assessment and revaluation of the current security posture of University- looked at configurations and decks. <u>Not penetration testing</u> . <u>3. Project: Large global telecommunications a streamlined penetration testing model</u> to aid the client in more penetration testing against all of their web applications, based on lower risk tolerance from the c-suite and new compliance demands after critical findings were identified in one of their web applications. Conduct penetration testing for OWASP Top 10 vulnerabilities and other web application flaws. Design and implement an end-to-end manual pen test "factory model" for the client, including reporting and remediation processes. <u>4. Technology Company providing Identity Operating System</u> : comprehensive penetration testing on the client's Identity Operating System platform, a secure platform to provide customer insights to the worlds leading media technology and information services, in line with the client's core business values of data security. Conduct penetration testing on the Identity Operating System platform for OWASP Top 10 and other vulnerabilities at a web app and infrastructure level. <u>5. Technology and communications provider</u> : penetration test and threat model of the client's online web applications, in-store applications, and kiosks, in response to recent security incidents. The client's retail store ecosystem enables sales representatives to make customer sales and address customer needs, and the client was rolling out enhanced technical and security hardening measures to its stores and sought a penetration test of the new environment before deployment. The outcome was identification of multiple vulnerabilities, including several critical-risk vulnerabilities, which could have resulted in MASSIVE fraud and compromise across 100's of retail locations. (Capacity appears significant based on these examples and summary information. Experience is good - don't see SCADA mainframe or think client which was requested in the RFQQ higher education and private companies)
Staffing (30%)	30.0	20.0	<u>1. Michele Myauo Managing Director and Senior Security Executive</u> - does not have experience in conducting penetration testing. 20 years experience in cybersecurity. <u>2. Mark Williams</u> , Technology Consulting Senior Manager business processes, systems implementation operations improvement not penetration testing experience of cybersecurity technical background. <u>3. Greg Conover Senior Security Manager</u> 13 years of information security and offensive security experience Has worked in federal and state government, CISSP, CEH don't see penetration testing experience. <u>4. Hokkeung Chu</u> , security focused career no penetration testing. <u>5. Thulani Shabanguwe, Security Manager</u> , penetration test lead application pen tests, APIs and infrastructure test no certifications, no years of pen test experience but hundreds of applications and over 1,000 vulnerabilities remediated. <u>6. Rob Hettinger</u> , Security Consulting Manager, penetration test manager lead tester testing web applications, APIs, and thick clients, worked on the communications provider sample project, CIAC Web Application penetration tester GWAPT, 5 years experience. <u>7. Laurel Desrosier</u> , Security Consulting Manager, vulnerability management of application and infrastructure, not a penetration tester. no certifications, no years experience. <u>8. Haley Pereira</u> , Security Consulting Consultant, 4 years experience, security scanning and threat modeling. No penetration testing experience. <u>9. Ian Nespolo Security Consultant</u> , penetration tester, Web application, infrastructure, thick client OSCP, GCIH, Pentest+ Security + no years experience in penetration testing. <u>10. Grant Buben, Security Consultant</u> , penetration testers and security consultant, web application API Network OSCP, Security +, Network+ TIA+ no years experience. Overall 10 Key personnel, 4 personnel have penetration testing experience but unclear the depth of their experience for two of the four, except for Rob has 5 years and Thlani has tested hundred of applications.
Qualifications Section Total Score	65.0	50.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	12.0	<b>Targets included one API interface and one application. The content and remediation steps are clear YES.</b> Separate sections for management and technical audiences; <b>Yes but pretty technical</b>  An executive summary that presents findings, conclusions and recommendations; <b>Findings yes - overall conclusions and recommendations No.</b>  Testing methodology and a description of procedures used - testing methodologies should be described at a level of detail so that they are re-creatable using screen prints as necessary; <b>yes</b>  All test results and findings, including identification of tests performed that did not identify issues; <b>Yes but no to identifying tests with no issues</b>  Ranked results with a standard rating scale (likelihood and significance) detailing the seriousness of each finding and remediation prioritization; <b>yes</b>  Detailed information about how each issue can be fixed and the level of effort to fix; <b>yes to how to be fixed but not level of effort</b>  A description of the implications or impact of not fixing each of the issues noted; <b>Yes</b>  <u>An overall assessment based on the work performed for each agency and/or government including strengths and opportunities for improvement. No</u>
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	62.0	
Evaluator Initials :			
Date:			
Question: labs and offices in many countries globally is mentioned numerous times. Are the all the resources including the people, the testing and the storage of information going to be in the United States?			

Affinity IT			
K689 - Security Assessment Services			
Vendor: Affinity IT			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit. 180 hours for this scope of work
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	21.0	In the description of the expertise of the firm on page 40 there is a focus on network security and penetration testing of networks and web applications. Also notes "We are 100% network security focused" During the past five years, Affinity IT has completed 48 security assessments, with 18 of those being performed over the last 12 months. We have the capacity to fulfill Washington State Auditor's requirements of performing an average of 1 audit per week. demonstrates capacity to do the work - not sure of the depth of these engagements. <u>1. local gov experience, City in California</u> internal and external network penetration testing also physical penetration testing which we don't do at this time. <u>2. local gov experience West Virginia</u> . internal and external vulnerability assessment. <u>3. Local gave. experience housing authority Chicago</u> . external and internal network penetration testing, internal network vulnerability scan, wireless, Social engineering. <u>4. Education</u> . network penetration test, phishing application security vulnerability report. <u>5. Local gov City New Jersey</u> . internal and external network vulnerability scanning and network penetration testing. Overall: heavy focus on network which is part of what is in the RFQQ, timing looks good at two weeks but not a heavy focus on actual application penetration testing and the different types of applications. Approach and methodology look good. Excellent government experience
Staffing (30%)	30.0	15.0	Clear he will be involved in all steps of the work that is good. <u>2. Konrad P. Gawronski</u> from the NJ National Guard Cyber Warfare Operations Center and brings a strong networking background. Mr. Gawronski designed and implemented the current Affinity IT Security Phishing Platform, and personally manages all campaigns. Mr. Gawronski will work with Mr. Fisher and Mr. McCormick and be responsible for information gathering, network scanning, security analysis and reviews, and documentation of findings. good certifications, packet manipulation, indicators of compromise, all good, Network scanning but <b>not penetration testing</b> and we do not do phishing on our audits. 3. <u>Michael J. McCormick</u> Mr. McCormick brings over 35+ years of IT and cybersecurity experience to each project. His expertise includes Critical Infrastructure Protection (CIP), and risk assessment. Mr. McCormick will work with Mr. Fisher and Mr. Gawronski and be responsible for information gathering, network scanning, security analysis and reviews, and documentation of findings. CEH and Good background in critical infrastructure Network scanning, preparedness and detection <b>internal and external network security and penetration testing</b> <u>4. Daven Ryerson</u> nd <u>etwork based penetration testing</u> recently joined our Affinity security team and brings additional IT and cybersecurity expertise to each project. Mr. Ryerson will work with Mr. Fisher, Mr. Gawronski and Mr. McCormick and be responsible for information gathering, network scanning, security analysis and reviews, and documentation of findings,. good certs - CEH Security+ and NCSP Network scanning a <u>5. Thomas J. Czerniecki</u> . has extensive experience in municipal management and is a veteran of over 23 years of public management and consulting experience. Mr. Czerniecki is our resident expert in public management and will assist in project planning, report generation, suggested remediations, and readouts. <b>No penetration testing</b> <u>6. Mr. MacPhee</u> is an undercover operations specialist and our lead consultant on red-teaming engagements. His expertise includes covert operations, intelligence gathering, surveillance, and counterintelligence. Mr. MacPhee will be responsible for assessing the physical security of IT related facilities. <b>No penetration testing</b> and we do not do physical security assessments. If we did or decided to include this he looks well qualified. Overall - SAO audits require a broader scope of work then network scanning and some network based penetration testing noted, vulnerability assessments, and web applications - we need experience in all types of applications including, thick, mainframe, OT etc. Heavy focus on network which is part of what our audits cover. manual penetration testing at exploit. Six staff and all involved and their roles are clear- three do not do penetration testing.
Qualifications Section Total Score	65.0	36.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	8.0	<p>The assessment included remote scanning of external servers network devices and web based applications; internal credentialed vulnerability scan- not a penetration test just scan results. The content and remediation steps are clear Yes. Separate sections for management and technical audiences YES;</p> <p>An executive summary that presents findings, conclusions and recommendations; Findings yes - overall conclusions and recommendations</p> <p>Testing methodology and a description of procedures used - testing methodologies should be described at a level of detail so that they are re-creatable using screen prints as necessary; Yes but these findings don't need screen shots</p> <p>All test results and findings, including identification of tests performed that did not identify issues; yes and no to identification of tests with no results</p> <p>Ranked results with a standard rating scale (likelihood and significance) detailing the seriousness of each finding and remediation prioritization; severity, yes but not defining what that means - the likelihood and significance matrix</p> <p>Detailed information about how each issue can be fixed and the level of effort to fix; yes but high level recommendation but appropriate for this level of finding</p> <p>A description of the implications or impact of not fixing each of the issues noted; Yes high level</p> <p>An overall assessment based on the work performed for each agency and/or government including strengths and opportunities for improvement. Yes in the executive summary but no strengths noted</p>
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	44.0	
Evaluator Initials :			
Date:			



K689 - Security Assessment Services			
Vendor: Berry Dunn			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit. 204 hours testing seems highly automated process.
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	16.0	Firm has been conducting vulnerability scanning and penetration testing for more than five years and security risk assessments for 10. consulting service has worked with a multitude of state and local governments. <u>Government territory Project 1:</u> penetration testing and vulnerability scanning on 5 web applications and 25 servers. Configuration assessment on server and database. <u>Project 2, county Government</u> . Penetration testing on 14 external web applications; <u>Government state Project 3:</u> vulnerability and penetration test of wireless network and wireless config, access, monitoring encryption. <u>State experience project 4.</u> Penetration testing complex applications and included a mainframe. <u>Project 5: government county experience.</u> vulnerability scan and penetration test including OSINT and credentialed attack could not access the SCADA. Overall Experience with most types of work we do but it is narrow and no SCADA testing (just attempted access), or OT testing. Penetration tests are on the narrowly scoped side. Only five years experience with penetration testing. Excellent government experience.
Staffing (30%)	30.0	15.0	<u>1. Bill Brown</u> ; 34 years of audit, cost accounting, financial consulting, and compliance assessment experience. oversee security assessments <b>No penetration testing experience.</b> 2. <u>Matt Bri</u> a security focused security analytics, enterprise resource planning security, network and cloud security, security architecture, security governance, risk assessments, and compliance. Matt is a certified Project Management Professional® (PMP®), Certified Information Systems Security Professional (CISSP), GIAC Systems and Network Auditor (GSNA), and PCI-QSA with 19 years of security-related project management experience <b>No penetration testing experience but oversees it.</b> 3. <u>Mitch Darrow security focused</u> GPEN 25 years of experience in business system analysis, database design, system architecture, network administration, and design engineering. He has provided leadership on technology projects to measure, analyze, and improve performance issues, training and development, project coordination, as well as strategy and planning for information technology projects related to human services. Conducts penetration testing and vulnerability assessments. 4. <u>Louis Krupp</u> , GSNA, CISSP, PIC QSA a senior consultant with Berry Dunn's Government Assurance Practice Area, focusing on assisting clients with IT security projects, with specific experience with MARS-E and PCI assessments. Louis brings a passion for penetration testing and vulnerability scanning to determine and reduce business risk currently working on a Penetration Testing with Kali Linux course to get his Offensive Security Certified Penetration Tester certification. Overall to managers, one with depth of knowledge in IT security and two penetration testers have broad experience in many areas related to IT security, policy review, documentation and evidence collection, PCI assessments, threat briefs, but also do penetration testing - Louis not doing penetration testing as the core or sole focus of work.
Qualifications Section Total Score	65.0	31.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	7.0	<b>Targets included an internet facing multi tier web application the beginning of the report is mostly scans, custom scripts many potential vulnerabilities identified but not confirmed, highly automated. The content and remediation steps are clear yes.</b> Separate sections for management and technical audiences; <b>Just Technical</b>  An executive summary that presents findings, conclusions and recommendations; <b>Yes</b>  Testing methodology and a description of procedures used - testing methodologies should be described at a level of detail so that they are re-creatable using screen prints as necessary; <b>YES, no screen shots</b>  All test results and findings, including identification of tests performed that did not identify issues; <b>all testing results yes those that did not find issues no</b>  Ranked results with a standard rating scale (likelihood and significance) detailing the seriousness of each finding and remediation prioritization;  Detailed information about how each issue can be fixed and the level of effort to fix; <b>some yes but mostly No</b> A description of the implications or impact of not fixing each of the issues noted; <b>some yes</b>  An overall assessment based on the work performed for each agency and/or government including strengths and opportunities for improvement. <b>No</b>
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	38.0	
Evaluator Initials :			
Date:			

BPM			
K689 - Security Assessment Services			
Vendor: BPM			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit. nothing to add just cost given.
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	21.0	local governments, state agencies and utilities. <u>Project 1: State agency</u> , Penetration test vulnerability remediation matrix. PSTN-facing services, web-facing services, email, internal network, phone controls. <u>Project 2: State agency</u> , same as first testing controls from information gathering, PSTN-facing services, web-facing services, email platform and inbound/egress controls, physical security controls, internal network, host, protocol and egress controls, as well as phone-based, phish, and in-person social engineering provided a comprehensive baseline of where controls were operating as intended and where they were either absent or ineffective. <u>Project 3 state public utility</u> : two web applications that two two weeks, one web application took three weeks. <u>Project 4: city-</u> m information gathering, PSTN-facing services, web-facing services, email platform and inbound/egress controls, physical security controls, internal network, host, protocol and egress controls, as well as phone-based, phish, and in-person social engineering provided a comprehensive baseline of where controls were operating as intended and where they were either absent or ineffective. Additionally, a SCADA assessment thoroughly analyzed their SCADA networks for performance, reliability, and security vulnerabilities SCADA <u>Project 5: Public Utility District -</u> information gathering, PSTN-facing services, web-facing services, email platform and inbound/egress controls, physical security controls, internal network, host, protocol and egress controls, as well as phone-based, phish, and in-person social engineering provided a comprehensive baseline of where controls were operating as intended and where they were either absent or ineffective. Additionally, a SCADA assessment thoroughly analyzed their SCADA networks for performance, reliability, and security vulnerabilities. the Cybersecurity Assessment Services team has performed over 1,200 comprehensive penetration tests and over 600 information security program reviews, configuration reviews and risk assessments (Overall: Good experience with state and local governments. raises questions of capacity - we usually do the entire test with 5-8 applications plus external and internal network in two weeks plus a week or two for reporting- project three notes web applications that two two weeks, one web application took three weeks. No mention of thick client or mainframe.) Firm has good certifications, CEH, CISA., CPT, CSSA, OSCP, OSWE, Security+
Staffing (30%)	30.0	17.0	<u>1. David</u> , advisory partner: Has lead over 1,200 inforamtion security assessment engagements and has worked in IT with governments, utilities, and healthcare for 25 years. <b>oversees the program no pentest</b> <u>2 Megan</u> project manager, keeping projects timely 5 years <b>no pentest</b> . <u>3. Joshua</u> , Lead technical assessor, systems administrator, now a systems specialist and assessorCEH and CPT. <u>4 Alex Program Assessor Manager</u> : communicate areas for improvement with public speaking and critical reasoning and insights into security processes and procedures and worked in IT security with government, utilities and healthcare for 21 years CISA <b>no pentest</b> . <u>5. Jacob coordinate operations</u> , support project management and account managers, and ensure the accuracy and timeliness of CSAS team results <b>no pentest</b> <u>6. Ryan</u> coordinate operations, support project management and account managers, and ensure the accuracy and timeliness of CSAS team results, CEH, certified SCADA architect. <u>7. Derek Senior Program Assessor</u> focuses on client program assessment activities; <u>8. Sam Z, Senior Technical Assessor</u> , penetration testing methodologies for conventional networks to WiFi OT and Cloud; <u>9. Jon P Senior Technical Assessor</u> leads the targeted Red Team Exercises Comp TIA pentest+ <u>10. Zach B. Senior Technical Assessor</u> knowledge of applications and their underlying infrastructure insight inot enterprise level infrastructure and the applicaitons used by those entities (Overall two people responsible for project management and coordination, one for communications; 6 of the 10 staff are titled "assessors", one is the managing assessor, assume those are all doing penetration testing not clear on their penetration testing experience similar to the work described in the RFQQ)
Qualifications Section Total Score	65.0	38.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	10.0	Targets included phishing, network devices, email servers, modems, physical sercurity a web application. The content and remediation steps are clear yes. Separate sections for management and technical audiences; <b>yes but pretty technical</b>  An executive summary that presents findings, conclusions and recommendations; <b>YES</b> .  Testing methodology and a description of procedures used - testing methodologies should be described at a level of detail so that they are re-creatable using screen prints as necessary; <b>YES</b>  All test results and findings, including identification of tests performed that did not identify issues; <b>Yes but not tests performed that did not identify issues</b>  Ranked results with a standard rating scale (likelihood and significance) detailing the seriousness of each finding and remediation prioritization; <b>YES- with a clear definition; Also provide Accept, Manage, elimatte for each finding</b>  Detailed information about how each issue can be fixed and the level of effort to fix; <b>YES but not level of effort</b> A description of the implications or impact of not fixing each of the issues noted; <b>YES</b>  An overall assessment based on the work performed for each agency and/or government including strengths and opportunities for improvement. <b>Yes and someoverall assessment</b>
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	48.0	
Evaluator Initials :			
Date:			

K689 - Security Assessment Services			
Vendor: CAI			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit. 563 hours - timeline is pretty long at 2 months one week, likely due to two penetration testers.
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	14.0	Firm has 387 resources providing direct support to clients in the US in roles related to security and security administration.86 % of the business is serving the public sector We provide both red team and blue team services for our clients. The spectrum of services includes traditional vulnerability assessments, network penetration testing, and web application testing. We also assess mobile applications and hybrid/cloud environments for vulnerability. (Note from evaluator: This is most of what we do but not all of what we do; they give an approach for SCADA OT but we do Thick clients and sometimes mainframe; noting they don't do manual penetration testing in their approach) <u>Project 1</u> : Waste Water district Penetration test network, confidential information with name of entity. <u>Project 2</u> , water district penetration test on network black box confidential details not included. <u>Project three</u> : Metra rail included testing on SCADA and OPT penetration testing. No confidential details included. <u>Project 4</u> : Florida based report external assessment of technology including penetration testing. Project 5: water district, very large, validate access management and identify unnecessary accounts used a PowerShell script and evaluated service account activity threat actor identified. <u>Overall</u> - all testing completed in the timeframe we could look for. Working with local governments. All testing includes penetration testing but the scope of the work is general and narrow then the work in the RFQQ, specifically not a lot of application testing including web, thick or mainframe, yes to SCADA and OT. <b>Lots of confidential information provided on two examples.</b>
Staffing (30%)	30.0	14.0	1. Rex Johnson, PMP, PCIP, CISA, CISSP, executive Director, 30 years experience, digital forensics. and IT audits and controls. Good cyber experience not a penetration tester. 2. Pedor Ortega, MSCIA, OSCP, CEH, CHFI, 20 years of cybersecurity and IT with government and energy other other private sectors. Red team and blue team. 3. Annie Liao, Security +, ISC CC, AWS CCP, 16 years IT support and troubleshooting. Two years penetration testing. Overall, two people with penetration testing experience, one only two years not depth in penetration testing. Pedro has a long IT background but not a long penetration testing background.
Qualifications Section Total Score	65.0	28.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	12.0	Targets included internal and external network services. they noted the entity in the report on page 22/40 in the table. The content and remediation steps are clear <b>YES</b> . Separate sections for management and technical audiences <b>YES</b> ;  An executive summary that presents findings, conclusions and recommendations; <b>Yes</b> .  Testing methodology and a description of procedures used - testing methodologies should be described at a level of detail so that they are re-creatable using screen prints as necessary; <b>YES screen shots and general methodology</b>  All test results and findings, including identification of tests performed that did not identify issues; <b>Yes but not tests that did not identify issues</b>  Ranked results with a standard rating scale (likelihood and significance) detailing the seriousness of each finding and remediation prioritization; <b>YES, also root cause or type of issue</b>  Detailed information about how each issue can be fixed and the level of effort to fix; <b>Yes Level of effort to fix is part of severity.</b> A description of the implications or impact of not fixing each of the issues noted; <b>Yes generally in the results ranking.</b> overall assessment based on the work performed for each agency and/or government including strengths and opportunities for improvement. <b>Yes to opportunities for improvement but not strengths.</b>
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	40.0	
Evaluator Initials :			
Date:			
Would like more information on this statement from page 16 of Exhibit D, "From our perspective, each project can experience schedule risk (i.e., delays) based on agency inaction. For example, with internal penetration testing, the agency is responsible for exposing certain aspects of their environment; we cannot proceed without this access. We use the ROE to delimit scope and define actions required by all parties."			



K689 - Security Assessment Services			
Vendor: Deloitte			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit. 798 hours seems high all testing done over two weeks seems good
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	21.0	Good experience with state and federal governments; provided a list of 13 penetration testers with credentials (four are key personnel and are noted in Staffing - Albert has good experience - One manager three testers of the three testers; Nicholle don't see penetration testing experience; David penetration test experience 4 years; Garrett some penetration testing 2 years; Jed Anderson 2 years experience; Christopher varied experience not clear on penetration testing experience; Ricky penetration testing 5 years.; Ayesha one year experience pentesting; Neel not clear on penetration testing but lots of other general cybersecurity roles; Victor six years experience pen testing ; noting many testers have other experience and are not just penetration testers so may not be testing as their main and focused career). performed security assessments for federal, state, and local agencies across the United States. <u>Project 1. Penetration testing</u> of an application at WA state agency with manual validation. Project 2: <u>Social Security Administration</u> : The scope consists of Wireless Penetration Testing, Network Penetration Testing, Web Application Penetration Testing, Red Team Operations (Adversarial Simulation), Purple Team Operations, and Vulnerability Assessments. reviewed tenable scan results indexed within Splunk to create dashboards. Conducted Red team and Purple team exercises to test security posture. <u>Project 3: State of Orgon Helath Authority</u> , vulnerability testing of ONE system, in addition to security regulatory compliance, identity and access management, web services security, security incident and event management, and data obfuscation- <b>Not penetration testing</b> . Project 4, South Carolina DHHS, Vulnerbility assessments. <b>Not penetration testing</b> <u>Project 5: State of Oregon, Information Support Services DHS</u> ; Penetration testing and vulnerability assessment - dynamic web applications, web servers and database servers (overall: Red team operations, two of the projects included narrow penetration testing and not clear of the scope of penetration testing vs vulnerbility scanning on project 5; not clear on the note that potential risk of false negatives being outside the vendor's control because in most cases penetration testing should rule out false positives)
Staffing (30%)	30.0	20.0	Four key personnel <u>1. Ian Flemming- Team Lead</u> : CISSP, CompTIA A+, Network +, internal external SCADA and ICS, <b>not a penetration tester, cybersecurity architect and IT management</b> <u>2. Keith Howell Penetration Tester</u> Certified Information Systems Security, Professional (CISSP)—ISC2,- Offensive Security Certified Professional (OSCP)—Offensive Security- Digital Forensics and Incident Response, penetration testing manager, government experience; Designed virtual software testing tools for classified environments. <u>3. Olu Afolabi</u> Security +, CEH and CISA; <u>4. Albert Tao Penetration tester</u> ; OSCPPerformed Webapp, Network, and Infrastructure pen testing of internal client network. Target network used a wide variety of technologies such as Amazon AWS, PostgreSQL, and a custom CMS by Kore.AI. Conducted in depth manual REST API testing. Scoped network and enumerated target hosts. High familiarity with a wide range of pen testing techniques and toolsets, both manual and automated. Extensive specialization in black box testing web applications, CMS exploitation, and data exfiltration. (overall don't see a lot of testing experience from Keith but impressive experience; Not clear on Olu depth of experience with testing in but it notes they do web applications and mobile applications, Albert has good experience - One manager three testers )
Qualifications Section Total Score	65.0	41.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	9.0	<b>Targets included network penetration test not clear if external or internal; likely external based on the description of purpose.</b> The content and remediation steps are clear Straightforward findings and remediation is straightforward. Yes Separate sections for management and technical audiences; <b>Yes but it was on the technical side</b>  An executive summary that presents findings, conclusions and recommendations; . <b>Yes.</b>  Testing methodology and a description of procedures used - testing methodologies should be described at a level of detail so that they are re-creatable using screen prints as necessary; <b>Methodology yes, no screen prints but not necessary</b>  All test results and findings, including identification of tests performed that did not identify issues; <b>Yes but not tests that did not identify issues</b>  Ranked results with a standard rating scale (likelihood and significance) detailing the seriousness of each finding and remediation prioritization; <b>Yes with root cause or type of issue</b>  Detailed information about how each issue can be fixed and the level of effort to fix; <b>Yes detailed information about how to fix but not level of effort to fix</b> A description of the implications or impact of not fixing each of the issues noted; <b>Yes well defined with impact</b>  An overall assessment based on the work performed for each agency and/or government including strengths and opportunities for improvement. <b>Yes the vulnerability by root cause but not the strengths</b>
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	50.0	
Evaluator Initials :			
Date:			



K689 - Security Assessment Services			
Vendor: Digitech			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit. . 695 hours. Timeline includes 30 days for attack simulation and 20 days for exploit development. timeline is long. high level methodology. Very detailed methodology attached.
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	30.0	Strobes Security has 6+ years of dedicated, niche experience in delivering high quality vulnerability assessments that includes web applications, thick client applications, mainframes, operational technology, network and source code review. Strobes Security has 6+ years of specialist experience in delivering high quality auditing and assessing wireless networks. <u>Project 1: US pharma.</u> Quarterly Network (5 Nos), Web (7 Nos), and Thick Client (3 Nos) Application VAPT Assessment Web Application VAPT - one-time assessment in a year (12 Nos) Source code reviews once a year (10 Nos of web, mobile apps) Penetration testing of medical devices (2 Nos) once a year. <u>Project #2 Europe-based e-commerce platform</u> that offers a range of products and services to customers worldwide. Quarterly Network (3 Nos), Web (10 Nos), and Mobile (5 Nos) Application VAPT Assessment Web Application VAPT - one-time assessment in a year (15 Nos) Source code reviews once in a year (12 Nos of web, mobile apps) Phishing assessment for employees (1 Nos) once in a year. <u>Project 3: oil and gas company</u> with refineries and production facilities. quarterly Network (7 Nos), Web (5 Nos), and Thick Client (3 Nos) Application VAPT Assessment Web Application VAPT - one-time assessment in a year (8 Nos) Source code reviews once in a year (5 Nos of web, mobile apps) ICS/SCADA Security Assessment (2 Nos) once in a year. <u>Project 4: telecommunications company.</u> Quarterly Network (12 Nos), Web (8 Nos), and Mobile (5 Nos) Application VAPT Assessment Web Application VAPT - one-time assessment in a year (10 Nos) Source code reviews once in a year (8 Nos of web, mobile apps) Social Engineering Assessment (1 Nos) once in a year. <u>Project 5: Government Australia responsible for national security and defense.</u> Quarterly Network (15 Nos), Web (5 Nos), and Thick Client (3 Nos) Application VAPT Assessment Web Application VAPT - one-time assessment in a year (7 Nos) Source code reviews once in a year (5 Nos of web, mobile apps) Red Team Assessment once in a year. (the scope of work in these projects matches the type of work we requested in the RFQQ. The last project is government related)
Staffing (30%)	30.0	20.0	<u>1. Bhushan Shinde,</u> compliance manager, 7.5 years experience in information security and risk management. <u>2. Prakash Ashok Team Lead.</u> OSCP AWS certified, three years in information security Web, Mobile, Network, API Vulnerability Assessment and Penetration Testing red team assessments. <u>3. Shiva Krishna Sr. security analyst and team lead.</u> 4 years experience in IT security. Web and mobile application testing, red team assessments, source code reviewer. Reported valid bug for 20+ companies including the US DOD. <u>4. Vatsal Agrawal Sr Security Analyst and team lead</u> OSCP CRTP 4 Years' experience in cyber security and he is well versed with, penetration testing techniques. He is CRTP, OSCP certified professional with experience in web app penetration testing, network penetration testing, active directory penetration testing and mobile app penetration testing, red team assessment. Red team assessments. (4 testers with good experience in penetration testing not clear on the role of strobes, are they contributing staff, it says they are a partner in the bidders profile)
Qualifications Section Total Score	65.0	50.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	8.0	<b>Targets included network penetration test.examples include red information</b> The content and remediation steps are clear <b>Yes.</b> Separate sections for management and technical audiences; <b>Yes</b>  An executive summary that presents findings, conclusions and recommendations; <b>No recommendations, yes to findings and conclusions - declare systems are moderately vulnerable.</b>  Testing methodology and a description of procedures used - testing methodologies should be described at a level of detail so that they are re-creatable using screen prints as necessary; <b>Yes</b>  All test results and findings, including identification of tests performed that did not identify issues; <b>Yes to findings but not tests that did not identify findings</b>  Ranked results with a standard rating scale (likelihood and significance) detailing the seriousness of each finding and remediation prioritization; <b>yes</b>  Detailed information about how each issue can be fixed and the level of effort to fix; <b>Yes no level of effort to fix</b> A description of the implications or impact of not fixing each of the issues noted; <b>Yes</b>  An overall assessment based on the work performed for each agency and/or government including strengths and opportunities for improvement. <b>Yes in risk evaluation, conclusions and recommendations no strengths noted</b>
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	58.0	
Evaluator Initials :			
Date:			

K689 - Security Assessment Services			
Vendor: EideBailly			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit. Very extensive detailed approach and methodology provided addressing each part of the scope. Appreciated the detailed description and would have liked to see more information about passive low touch testig on SCADA but the device assessment in the lab is interesting. Timeline is 1-3 weeks, good timeline.
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	21.0	Certifications do not include penetration testing but CISM, CISSP, CISA, GIAC and CRISC. Cybersecurity is an outsourced and managed service. more than 1,100 government clients firmwide. <u>Project 1: Idaho Housing and Finance</u> : Internal vulnerability Assessment external penetration testing. <u>2. Children's Miracle Network</u> : Internal vulnerability assessment, external penetraiton testing and web application testing. <u>3. Simi Valley school district</u> : Internal vulnerability assessment and external penetration testing. <u>4. Delta Dental Minnesota</u> : internal vulnerbility assessment, external penetration testing and web appcliaiton testing. <u>5. College of Western Idaho</u> . Internal vulnerability Assessment, external penetration testing, web appicaiton tesing. Overall these tests seem narrow, many of tests include different types of applications internal and external applications and network testing.
Staffing (30%)	30.0	15.0	<u>1. Cybersecurity Practice Leader, Kyle Hendrickson</u> will oversee the engagement background in cybersecurity <b>not a penetration tester</b> ; <u>2Anders Erickson</u> will serve as the Risk Advisory Principal, IT Auditor <b>not a penetration tester</b> . <u>3.Dale Lozo</u> , Senior Manager, IT security professional and leader not a <b>penetration tester</b> <u>4 Rob Else</u> , Manager, will serve as Cybersecurity Specialist. Cybersecurity professional focus on healthcare <b>not a penetration tester</b> . Overall, difficult to assess extent of penetration testing experience in relation to the types of experience we are requesting in the RFQQ
Qualifications Section Total Score	65.0	36.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	9.0	Targets included Internal vulnerability assessment. The content and remediation steps are clear Yes . Separate sections for management and technical audiences; One very short executive summary lots of technical information An executive summary that presents findings, conclusions and recommendations; Yes not recommendations. Testing methodology and a description of procedures used - testing methodologies should be described at a level of detail so that they are re-creatable using screen prints as necessary; YES All test results and findings, including identification of tests performed that did not identify issues; Yes not tests that did not identify issues Ranked results with a standard rating scale (likelihood and significance) detailing the seriousness of each finding and remediation prioritization; Yes Detailed information about how each issue can be fixed and the level of effort to fix; Yes not level of effort to fix A description of the implications or impact of not fixing each of the issues noted; Yes <del>An overall assessment based on the work performed for each agency and/or government including strengths and opportunities for improvement</del> Yes overall conclusions and recommendations No strengths identified
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	45.0	
Evaluator Initials :			
Date:			



K689 - Security Assessment Services			
Vendor: Emagined			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit. 176 hours level one testing - this level of hours seems low for this size engagement. EMAGINED testing is designed to be exhaustive, which means that the team will not stop at the first successful penetration but will continue to identify all vulnerabilities and attack vectors. 5 testers one coordinator. five weeks timeline looks okay.
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	33.0	Emagined Security has over 40 consultants with extensive information security backgrounds. Of those 40 consultants, 20 have capabilities to perform penetration testing, 12 are full time penetration testers. All have extensive experience with state and local governments. Emagined Security employees over a dozen penetration testers and can staff multiple engagements of this size (sample in quotation) simultaneously. This is a dedicated penetration test team and current members have been background checked by the State of Washington including CJIS certification and undergone Washington State Patrol fingerprint background checks. Emagined Security has been performing Vulnerability Assessment and Penetration Testing for over 22 years. Our more experienced team members have been performing penetration testing and ethical hacking engagements for over 30 years. All penetration testers are required to acquire at least one additional certification per year to ensure skills are up to date Emagined Security performs hundreds of Web Application Penetration Tests, Network Penetration Tests, API & Mobile Penetration tests, Mobile, Secure Code, Mainframe, Vulnerability Assessments and Wireless Assessments every year. This type of testing continues to be a core service Emagined Security offers. Long list of certifications including penetration testing certifications. methodology is similar to the methodology prescribed in this document and in Exhibit C, with limited dependence on automated scanning. <u>Project 1: 4weeks</u> . 6 Web application Penetration Tests, 1 Thick Client Penetration Test, SCADA Testing of 25 systems, External Network Penetration Testing of 50 IP addresses, Internal Network Penetration Testing of 1,200 IP addresses and a Firewall Review. 8 resources assigned each roll is clear and involved in the work <u>Project 2</u> : WA state hospital scope included 4 Web application Penetration Tests, 2 Thick Client Penetration Test, IoT Testing of 2 subnets of sensitive medical equipment, External Network Penetration Testing of 20 IP addresses Internal Network Penetration Testing of approximately 2,000 IP addresses Firewall Review OSINT Review; 3 weeks; 7 staff and roles are clear and all involved in testing oversight and guidance <b>identified a new zero-day vulnerability that required our penetration tester to build custom code to prove the exploit.</b> <u>Project 3</u> : Open-Source Intelligence review (OSINT) and External penetration test for a Critical Infrastructure (CI) Organization located in Washington State, two weeks and two staff. Project 4: Emagined Security performed multiple application and infrastructure penetration tests at hospitals and infrastructures managed / operated by a hospital management company. This penetration testing is required to assist in the protection of HIPAA data. <b>An indicator of compromise was identified and confirmed.</b> Two staff and four weeks; <u>Project 5</u> : perform a penetration test for a Global Software Vendor with a market cap of 13B, six web applications, external network 12,000 IP addresses, internal network penetration testing 40,000 IP and segmentation testing of 12 networks, 12 weeks seven staff (Overall roles are clear: Principal penetration tester (15 years experience) assigns testers and Senior penetration (10 years experience )tester follow up with each tester 5 years experience to ensure questions and consolidate findings; every project includes penetration testing including the different types of applications, thick and web and OT and SCADA and some tests were very extensive. time lines are good, some government experience)
Staffing (30%)	30.0	28.0	<u>1. Patrick Cleary</u> , Executive Security Consultant, extensive certifications. Lead tester and trainer on hundreds of penetration testing engagements, including a social engineering exercise complete with pivot and advancement protocols and behavioral pattern analysis, as well as coordinator and program lead for annual global security assessment efforts which conducted network penetration testing at a macrolevel on both external and internal enterprise assets totaling in excess of 6500 systems and applications. • Highly skilled technical lead with demonstrated expertise in web application, thick client, API, WebSocket, mainframe, and embedded applications as well as networks and critical infrastructure, including ICS/SCADA. Performed during his 25+ years in cybersecurity overdo 500+ network penetration tests 500+ web application penetration tests 300+ API penetration tests 150+ thick client penetration tests 100+ ICS/SCADA penetration testso 50+ Mainframe and specialized penetration tests. <u>2. Ramcés Chirino</u> , extensive certifications Principal Consultant, Lead tester on over 400 penetration testing engagements, including web application, thick client, API, embedded devices and network and critical infrastructure based o has performed during his 20+ year career: 600+ web application penetration tests 400+ network penetration tests 300+ API penetration tests 200+ thick client penetration tests. <u>3. Arthur Borrego, Principal Consultant</u> Lead tester on over 300 penetration testing engagements. Has performed during his 10+ year career: 300+ web application penetration tests 300+ network penetration tests 100+ API penetration test 70+ thick client penetration tests Achieved “Guru” status and ranked in the top 100 in the “Hack The Box” penetration testing labs, which is a well-known educational platform for ethical hacking. <u>4. Felix Alcalá, Senior Consultant</u> , extensive certifications Offensive Security Engineer with over two decades of experience in Information Technology. He specializes in identifying and exploiting software vulnerabilities 2700+ penetration tests, encompassing all facets of network, mobile, and application penetration testing. made notable contributions to the MASV (Mobile Application Security Verification Standard) and MASTG (Mobile Application Security Testing Guide) projects of OWASP (Open Web Application Security Project). <u>5. Cory Dixon, Senior Consultant</u> , CEH, PGP certifications Lead penetration tester on over 400 application and network-based penetration tests, including mobile applications and embedded devices as well as web application, thick clients, APIs and network based/critical infrastructure. <u>6. Dom Allen, Senior Consultant</u> . SLAE, SPSE, SJSE, PCNSE, CCNA (R&S),Pentest+,CySA+, Sec+, Net+, A+ has conducted over 200+ application and network-based penetration tests during his 6+ year career. <u>7. Ishmael J. Malik, Senior Consultant</u> . Lead penetration tester on over 400 engagements, including various web application, API, thick client, and network-based penetration tests, including mainframe and ICS/SCADA. Certified Ethical Hacker CompTIA A+ Certification. <u>8. Yosbel Yanta, Senior Consultant</u> . Mr. Yanta has conducted over 50 network-focused penetration tests, and has lead several OSINT discovery efforts and web application penetration tests. CCNA, CCNA Security (Expired)CompTIA A+, N+, Security+; <u>9. Joe Nay, Senior Consultant</u> ; 4 years on the penetration test team performed over 100 penetration tests on networks, applications, and APIs, delivering detailed vulnerability analyses, related business impact, mitigation techniques, and expertise on overall security posture. CEH. <u>10. Aruna Sri, Senior Consultant</u> , (9) years of IT experience with dedication placed on penetration testing, security assessment, and automation testing. Lead OSINT investigator for Emagined Security, conducting over seventy-five (75) OSINT discovery efforts. • Web application penetration tester who has logged more than 100 web application penetration tests with several thick client and API tests.CEH. <u>11. David Ige, Security Consultant</u> Mr. Ige has performed over 150+ penetration tests on infrastructure and applications during his 6+ years career compTIA Network + and Security +. <u>12David Solarte, Security Consultant</u> . has performed more than 50 network penetration (overall, deep bench of penetration testers with a lot of experience with all types of penetration testing, every staff has experience in penetration testing and the most senior staff have the most penetration testing experience, would not be concerned could not do multiple engagements at once, last two staff have few certifications)
Qualifications Section Total Score	65.0	61.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item “d.” under “Report Results” on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	13.0	Targets included <b>external and internal network penetration testing and one application</b> . The content and remediation steps are clear . Separate sections for management and technical audiences; <b>pretty technical but yes</b>  An executive summary that presents findings, conclusions and recommendations; <b>Yes recommendations are in areas for improvement findings on page 7,8 and 10 . In the section next to executive summary, high level would improve the executive summary</b>  Testing methodology and a description of procedures used - testing methodologies should be described at a level of detail so that they are re-creatable using screen prints as necessary;  All test results and findings, including identification of tests performed that did not identify issues; <b>Yes but not tests that did not identify issues</b>  Ranked results with a standard rating scale (likelihood and significance) detailing the seriousness of each finding and remediation prioritization; <b>Yes</b>  Detailed information about how each issue can be fixed and the level of effort to fix; <b>Yes</b> A description of the implications or impact of not fixing each of the issues noted; <b>Yes, good descriptions</b>  An overall assessment based on the work performed for each agency and/or government including strengths and opportunities for improvement. <b>YES</b>
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	74.0	
Evaluator Initials :			
Date:			



ERM

K689 - Security Assessment Services			
Vendor: ERM			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <b>This is done by contract manager.</b>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit. 240 hours seems low but approach is well described and thorough. page 6or25- Reverse engineering code of application, <i>if allowed</i> . SCADA testing good approach and thorough. Two weeks is a good timeline.
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	30.0	Clients range from global multinational companies to small businesses, and include federal, state, and local governments and agencies, colleges and universities, transportation, financial services, healthcare, hospitality, technology, and many other industries. has performed Penetration Testing Services for more than 20 years, we are deeply experienced in the scope of work to be performed and fully committed to exceeding your expectations. We have performed vulnerability assessments and penetration tests for many local governments and agencies of different sizes and complexities. All of our project team members (including staff) have master's degrees in information technology, cybersecurity or related fields from some of the nation's most prestigious institutions and have some of the highest certifications in our profession. These certifications include CISSP, CISA, CRISC, CIPP, CISM, CIA, CJEH, PCI QSA, PCI PFI, CPA and many others. various types ranging from network, wireless, application, mobile devices, and SCADA. <u>Project 1 Miami-Dade County Finance Department</u> : Segmentation Penetration testing various county departments such as Aviation, IT, Cultural Affairs, Transportation and Public works, Fire Department, Water and Sewer, Solid and Waste Management, etc. and internal and external network penetration testing for the IT department (4 months each year) <u>Project 2: Metropolitan Washington Airport Authority</u> , highly technical network vulnerability assessments and penetration tests, 4 months but also include audits. <u>Project 3, Assurant</u> : PCI DSS and network penetration services for Assurant since 2014. Penetration testing services for Assurant encompass several regions such as Europe, Latin America and the United States. A specific project performed last year included the following assessments: - Internal Penetration Testing (North America and Europe) – total of approximately 1000 IP addresses Europe PCI DSS environment Segmentation Analysis- External Penetration Testing (North America and Europe) – approximately 1200 IP addresses- Penetration testing to the devices used to provide segmentation and analysis of the results. The time it took to complete this specific project from 2022 was five (5) weeks, deliverables included reports for each of the tests performed. 5 weeks <u>Project 4 City of St. Petersburg</u> : Perform a comprehensive PCI DSS audit. - Perform a cybersecurity audit using the CIS critical security controls. Review cybersecurity policies and procedures and perform a detailed analysis of the City's cybersecurity posture. - Perform Internal and external penetration testing of the City's networks including: Internal networks (wired and wireless LAN) External networks (wired and cellular WANS) Servers and appliances Endpoints Web Applications Perform Tabletop Exercise based upon the findings of the previous 3 areas. six months. <u>Project 5 Criminal Justice Coordinating Council</u> : The Criminal Justice Coordinating Council Penetration Testing Services on the JUSTIS Information Portal (web application) and the JUSTIS Exchange which included:- Simulating security breaches to test the relative security of computer systems, networks and applications.- Identifying areas that require physical protection of systems, servers and other network devices.- Pinpointing methods and entry points that an attacker may use to exploit vulnerabilities or weaknesses.- Searching for weaknesses in common software, web applications and proprietary systems.(overall examples of the types of systems applications and devices we test except not calling out mainframe or thick client. Every project has a substantial scope, most included other services in addition to penetration testing so timeline for just penetration testing is not 100% clear but looks generally good)
Staffing (30%)	30.0	25.0	<u>1. Esteban Farao, Director of Consulting Services</u> and with over 25 years of experience in security assessments, penetration testing and IT consulting services would be the Director for this project. Esteban has been performing all types of penetration tests for decades and for hundreds of clients in many industries He performs computer forensics and incident response during major security breaches. As an expert certified ethical hacker, he knows the routes malicious actors use to penetrate organizations and puts this knowledge to use to protect clients. His deep knowledge of computer forensics has helped him break open major cases related to fraud, embezzlement, IP theft and other misdeeds. has led >10k projects related to general data breaches. significant certifications. Determined that a bank employee copied a database to run a large identity theft operation. – Determined who processed \$2 million dollars of unauthorized wire transfer transactions via an on-line banking system by installing a malicious program in the administrator's machine. <u>2. Chris Sanchez</u> : Senior Information Security Manager. Performs penetration testing, digital forensic investigations, and data breach investigations for the firm's diverse client base, including the banking, legal, government and retail industries. His training in reverse malware engineering, incident response, detection and eradication of threats, and advanced digital forensics equips him to battle data breaches in a technically legally-sound manner. external / internal /wireless penetration testing, web application penetration testing, Chris also has six years of experience leading penetration testing, social engineering, and compliance assessments for ERMProtect, certifications are EnCase Certified Examiner, PCI forensic, reverse malware engineering and communicator Coin holder <u>3. Senior Consultant Divyansh Arora</u> conducted hundreds of vulnerability assessments of 100 plus web applications, IPs in the network, Android & iOS mobile applications and IoT devices such as CCTV and Central Command displays, for multiple government and private clients. He also assessed various phases in the SDLC and performed static and dynamic source code reviews. Discovered possibility of fraud payments in payment gateway applications and prevented significant monetary losses to the client, ISCP and <u>4. Staff Consultant Collin Connors</u> develops the company's proprietary tools, such as our automated phishing and phishing-detection tools. He oversees the company's internal security to prevent attacks on our networks, utilizing penetration testing, monitoring logs and security software, including vendor software that analyzes our metadata to assess potential compromises. A Ph.D. candidate at the University of Miami, he is researching the use of AI to detect malware, implementation of blockchain at banks, and prevention of attacks in a shared cloud environment. Performed Internal, External, Wireless and Web application penetration tests for clients and for ERMProtect to secure infrastructure, systems, and data. no certifications Created automated tools to improve test performance. and <u>5. Aviral Sharma</u> . He performs risk assessments, data compliance assessments, and penetration testing for the company (overall 5 highly trained penetration testers but Aviral experience appears very new. Impressive that the Director of Consulting has a strong security and penetration testing background, don't see clearly these staff have done SCADA, or thick clients).
Qualifications Section Total Score	65.0	55.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	11.0	Targets included <b>internal network security penetration test, also clearly stated what was out of scope which is nice</b> . The content and remediation steps are clear <b>yes</b> . Separate sections for management and technical audiences; <b>Yes, separate reports</b>  An executive summary that presents findings, conclusions and recommendations; <b>YES well described</b> .  Testing methodology and a description of procedures used - testing methodologies should be described at a level of detail so that they are re-creatable using screen prints as necessary; <b>Yes and it references Appendices with information gathered and port scanning results but they are not included here</b> .  All test results and findings, including identification of tests performed that did not identify issues; <b>Yes but not tests that did not identify issues</b>  Ranked results with a standard rating scale (likelihood and significance) detailing the seriousness of each finding and remediation prioritization; <b>YES</b>  Detailed information about how each issue can be fixed and the level of effort to fix; <b>Yes detailed information to fix but not level of effort</b> A description of the implications or impact of not fixing each of the issues noted; <b>Yes</b>  An overall assessment based on the work performed for each agency and/or government including strengths and opportunities for improvement. <b>not strengths but overall general comment about issues and how to fix, not a general assessment</b>
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	66.0	
Evaluator Initials :			
Date:			

GSG

K689 - Security Assessment Services			
Vendor: GSG			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <b>This is done by contract manager.</b>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit. 875 hours . "GSG proposes a 2% annual escalation for the proposed hourly bill rates from the second year to provide the most competitive pricing for the entire contract duration." The approach is very well described and very detailed with reasoning behind all the steps and different use of tools at different steps- Many tools used at each step. It is great that the OSINT is the first part of the penetration testing proces. Note they are using custom scripts right from enumeration phase.SCADA testing approach looks thorough
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	32.0	Our attackers used a broad range of commercial and public tools from our well-maintained Virtual Security Test Center as well as manual methods <u>Project 1. US Department of Agriculture</u> , GSG conducted Operational Risk Assessments, Penetration Testing, Web Security Assessments with High Value Applications (HVA), and Red Team Assessments for all USDA offices and data centers nationwide and provided extended assessments for the for the Office of the Chief Financial Officer and National Finance Center (USDA–NFC), which processes payroll for over 600,000 federal government employees, four months; three staff. <u>Project 2: US Dept of the Treaury, OIG</u> , conducted penetration testing on web applications, including testing the strength of the session credential used by the web application, strength and proper logic flow of server executables, strength of the login and authentication process against common exploits, and other tests. Conducted internal and external penetration testing based on passive information gathering and network mapping, as well as active network scanning, one year two resources. <u>Project 3: Lansing Board of Water and Light</u> , GSG provided penetrating testing and digital forensic examination of the computing environment to: Assist in the identification of any indicators of compromise not otherwise detected by existing deployed cybersecurity tools.Performed remediation of all detected malware and inoculating the environment against reinfection where possible. SCADA assessment including governance, exclusive SCADA controls, data and application security, system assurance, monitoring controls and peripheral controls. performed wireless security testing and focused on enumerating and verifying potential attack vectors and threats to LBWL wireless infrastructure. Timefram is three years but expansive project beyond penetration tesitng and two resources. <u>Project 4. Fort Wayne Allen County Airport Authority</u> , External Network Vulnerability and Penetration, Internal Network Vulnerability and Penetration Testing Testing two resources. Internal and Web Application Assessment – Review the security level of FWACAA's local and cloud-based applications including the accessibility both internally and externally to test the application security and code vulnerability. Review the FWACAA's local servers for vulnerabilities. • Firewall and VLAN Testing - Gain a better understanding of potential corporate network vulnerabilities that may be visible from the Internet and to identify VLAN segregation weak points.Wireless assessment. two resources four months other services provided. <u>Project 5 State of Kansas Office of Information Technology Services</u> , large security project focused on security planning design, incident response and review but included pentration testingof an open source, highly configurable comprehensive surveillance and outbreak management application and vulnerability testing. This is a contract providing CISO support personnel <b>Project ongoing is 5 years and does not end till 2024</b> . Provided extensive list of state, federal local and education organizations provided services to - great government experience. (Overall each project includes penetration testing, some large scope, and a other IT security services, testing includes most of the types of applications SAO includes in the RFQQ but I dont see specific mention of thick client; not clear on the number of resources on each project as it shows staff that worked on the projects but those may have been the leads, one project is ongoing)
Staffing (30%)	30.0	22.0	1. Vicki Shah: For over 15 years, Ms. Shah has been on Global Solutions Group's Contract and Project Manager for large IT programs, including those for city, state, local, and federal government agencies. Oversees, directs and assists with penetration testing. Extensive experience managing projects for local, state and federal government, which include penetration testing. <u>2. Vatsal</u> over 20 years in information technology and operations. He possesses proven technical skills in network technologies, operating system platforms, and IT infrastructure security controls. Mr. Shah's specialty skills involve vulnerability assessment and penetration testing with a focus on secure network architecture, 802.11x (Wi-Fi), web application portals, and physical security. Mr. Shah has extensive experience with CJIS, NIST, PCI compliance. He has also performed assessments of regulatory compliance with the Heath Insurance Portability and Accountability Act (HIPAA) and Sarbanes-Oxley (SOX). He has designed and implemented security architecture for product testing environments and operational use. His security architecture design experience includes firewalls, intrusion detection systems, virtual private networks (VPNs), cryptographic systems, authentication mechanisms, and multiple-tier web applications. Performed over 100 web application assessments and network penetration tests for commercial organizations. Extensive government experience. Extensive certifications. <u>3. Kumar</u> ; more than 15 years of experience in providing penetration testing in multiple sectors including university, healthcare, finance, and technology sectors. highly adept in developing and implementing security, privacy, and breach management programs with expertise in vulnerability assessment and penetration testing. In-depth knowledge of security assessments of databases, EHR/EMR, SAP, Oracle Financials, and other ERPs with eight years of experience in performing security and privacy risk assessments and audits. Well-versed in HITRUST SOC 1/2/3, FFIEC,NIST, COBIT, HIPAA, PCI-DSS, SEI-CMM methodology, IT QA methods, and ISO security standards with vast understanding of threat modeling using frameworks such as Octave Allegro and MITRE ATT&CK. extensive certifications. CISO for Halo Investing, current. (overall: staff have very good experience but only three staff)
Qualifications Section Total Score	65.0	54.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item “d.” under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	15.0	<b>Targets included external network and external web applications.</b> The content and remediation steps are clear <b>YES, very</b> . Separate sections for management and technical audiences <b>YES</b> ;  An executive summary that presents findings, conclusions and recommendations; <b>Yes</b> .  Testing methodology and a description of procedures used - testing methodologies should be described at a level of detail so that they are re-creatable using screen prints as necessary; <b>Yes</b>  All test results and findings, including identification of tests performed that did not identify issues <b>Yes to both the executive summary notes many passive results noting vulnerabilities that were evaluated for and not found</b> ;  Ranked results with a standard rating scale (likelihood and significance) detailing the seriousness of each finding and remediation prioritization <b>Yes</b> ;  Detailed information about how each issue can be fixed and the level of effort to fix <b>Yes</b> ; A description of the implications or impact of not fixing each of the issues noted <b>Yes well defined</b> ;  <b>An overall assessment based on the work performed for each agency and/or government including strengths and opportunities for improvement. Yes this was included in the Executive Summary</b>
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	69.0	
Evaluator Initials :			
Date:			
GSG has a strategic partnership with Google   Mandiant who will serve as subcontractors on our team love to hear more about what Mandiant's role is, it looks like all the staff are with GSG			



K689 - Security Assessment Services			
Vendor: Guidepost			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit. 160 hours seem like a low estimate for this size of scope. (lots of information about project management. not clear on identifying and prioritizing the state agency local governments IT security posture and developing an initial agencies/government focused list - it makes me think the project is misunderstood.) When an organization determines the scope, they often define a smaller attack surface than the one the attackers can find. If a discovery operation of the actual attack surface is not performed, the pen test might leave critical vulnerabilities undiscovered- OSINT is included as first step. The description of the approach is general and not specific to the scope of work.
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	21.0	Guidepost is a full-service technology firm, providing security consulting and design services to assess and address cyber security, safety, and communication needs. We specialize in IT network, cyber security and assessments, penetration testing, security systems design, site security design, conducting security assessments, evaluating security practices and associated risks, and providing recommendations and prioritizing needs. Guidepost has served more than 60 California cities and counties and have conducted security system assessments at more than 1,000 facilities, including utility and water district facilities, critical infrastructure sites, administrative buildings, laboratories, courthouses, detention facilities, and hospitals. (Overall good experience with state and local government; lots of firm certifications but not penetration testing related) <u>Project 1: Little rock conversion and visitors bureau</u> : a thorough assessment along with two (2) reports that detailed the current vulnerabilities, network components, along with best practices and recommendations for immediate and long-term remediation ( <b>not clear on scope of penetration testing</b> ) <u>Project 2: Los Angeles County office of education</u> : a site assessment and a network performance test to ensure that the existing network is efficient and to identify potential gaps. The findings and road map of recommendations helped to facilitate and shape a design in support of electronic security systems enhancement and upgrade. The scope of work also included network and telecom infrastructure design and consulting. ( <b>not clear on scope of penetration testing</b> ) <u>Project 3: Lee County Airport threat, vulnerability, and operational assessment (TVA) for the Southwest Florida International Airport, in Lee County, FL.</u> We are deploying a holistic planning approach and a comprehensive risk assessment methodology to address the unique security needs and challenges for the airport - <b>looks like a fully scope of the entity but not clear how big the penetration testing scope was whether internal external etc.</b> <u>Project 4: homeland security port of Richmond, California</u> , threat, vulnerability, and operational assessment (TVA) for the Southwest Florida International Airport, in Lee County, FL. We are deploying a holistic planning approach and a comprehensive risk assessment methodology to address the unique security needs and challenges for the airport <b>this looks like a very large scope of work, not clear on penetration testing scope.</b> <u>Project 5: California Department of Technology</u> . conduct the CDT Business Continuity Risk and Vulnerability assessment in 2016, 2018, 2020, and again in 2022. These assessments were conducted in accordance with the methodology described in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, Risk Management Guide for Information Technology Systems, in conjunction with NIST SP 800-53A, Assessing Security and Privacy Controls in Federal Information Systems and Organizations. The process included intrusion detection/penetration testing, Additional tasks included a review of existing security systems and master plan; and condensed security master plan and conceptual design <b>large scope and penetration testing but not clear on what or type assets, external internal in scope. Great experience with state, federal and local government</b>
Staffing (30%)	30.0	12.0	<u>1. Ahmad</u> : engineer and project manager, handling a broad range of projects from inception to completion <b>no penetration test experience</b> but areas of expertise include security and network. <u>2. Ken</u> : cybersecurity subject matter expert in policies and procedures. engineer and project manager, handling a broad range of projects from inception to completion CISSP and CISA, <b>not a penetration tester</b> <u>3. Alex</u> : 12 years of physical, Wi-Fi and cyber security experience to Guidepost's Security and technology Consulting practice. expertise includes enterprise-level security systems for critical infrastructure clients, access control and video systems, cybersecurity services including hardening networks, servers, endpoint devices, and vulnerability and penetration testing on networks to fully assess security risks. managed pre-deployment testing, documentation, and standardization phases for numerous enterprise technologies, as well as developing and managing effective deployment strategies. <b>has penetration testing experience not clear the depth</b> <u>4. Steve</u> : Steve Longoria has over 41 years of progressive and highly successful experience in assessing, designing, and deploying safety, security and emergency management projects and systems in the public and private sectors, including water systems. He is certified with the Sandia Risk Assessment Methodology-Water and designed and facilitated a "How to Conduct a Public Water System Security Vulnerability Assessment" Course for the City of Fairfield Water System Operators. <b>I don't see penetration testing</b> is the only person in Department of Defense history officially recognized as top expert in three different career classifications: Antiterrorism, Security & Safety's areas of expertise include safety and security, emergency management, strategic planning, and training and exercise <u>5. Rick</u> : diverse team leader with over 24 years of information systems expertise. He designs IT systems into comprehensive business enablers to develop resilient service availability to maximize production and productivity. <b>not a penetration tester no certs</b> <u>6. William Suthers</u> is the Director of Technical Services at Truventus and an open-source security tool developer, security researcher, and security conference speaker, including HushCon and DEF CON.Mr. Suthers has over fifteen years of security assessment and consulting experience with various industries, including security, SCADA, healthcare, government, military, small and large businesses, fiduciary and non-profit. 24 years of information systems expertise. He designs IT systems into comprehensive business enablers to develop resilient service availability to maximize production and productivity not a penetration tester <b>a penetration tester not clear on depth</b> <u>7.Jeff</u> : Jeff Hall has over thirty years of experience in information technology, information security and IT governance. He started his career as an IBM systems programmer writing and supporting operating systems, moved into application development, enterprise project management, CIO roles, CISO roles and then started a multinational consulting firm's information security and PCI practices. Mr. Hall's expertise ranges from operating systems to networking, enterprise application suites, information security and the cloud. He has been involved in a variety of projects to develop and implement innovative applications and services for small and midsize businesses to the Fortune 100. He has worked with manufacturing, distribution, financial institution, insurance, health care, and government organizations <b>Not a penetration tester</b> . <u>8.Jesse</u> : Jesse Hassett is a lifelong technologist dedicated to the intersection of technology and security. Jesse has been working in high technology for nearly 30 years. He has securely architected and implemented ISPs, built and operated financial systems, and maintained large scale machine learning systems. Drawing on his depth and breadth of experience helps him quickly understand technical details and focus on client needs (overall: Very high level of experience and expertise in cybersecurity but not clear on how much penetration testing and the types of testing we listed in the RFQQ)
Qualifications Section Total Score	65.0	33.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	7.0	<b>Just provided a table of contents do to the length so all assessments are based on limited information. Targets included comprehensive penetration testing</b> . The content and remediation steps are clear <b>unable to score</b> . Separate sections for management and technical audiences; <b>Yes to technical and management assuming the "narrative is management"</b> ..  An executive summary that presents findings, conclusions and recommendations; <b>Yes</b>  Testing methodology and a description of procedures used - testing methodologies should be described at a level of detail so that they are re-creatable using screen prints as necessary; <b>Yes</b>  All test results and findings, including identification of tests performed that did not identify issues; <b>Yes to finding issues</b>  Ranked results with a standard rating scale (likelihood and significance) detailing the seriousness of each finding and remediation prioritization; <b>Yes</b>  Detailed information about how each issue can be fixed and the level of effort to fix; <b>do not see remediation or recommendations related to each time of assessment</b> A description of the implications or impact of not fixing each of the issues noted; <b>don't see this</b>  An overall assessment based on the work performed for each agency and/or government including strengths and opportunities for improvement. <b>don't see this</b>
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	40.0	
Evaluator Initials :			
Date:			
5 staff are subconsultants			



K689 - Security Assessment Services			
Vendor: Inspira			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. <b>Please add comments as you see fit. 1035 hours over four months is on the long side - significant testing noted in approach Good approach and methodology each type of testing completed is well explained and very thorough - web app, mobile app, network testing, thick client etc</b> - conduct customized tests based on technology and business logic; the entire pen test will be carried out by our skilled and certified security engineers. Our senior penetration testing engineer will perform a detailed risk assessment on the vulnerabilities found, carefully weed out false positives and assign a scoring system based on CVSS (Common Vulnerability Scoring System) on to the findings
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	32.0	<u>Itegriti corporation</u> offers a range of strategy, analysis, and implementation services and has extensive experience protecting some of the nation's most critical infrastructure assets. Since 2006, they have provided OT/ICS compliance services, including NERC CIP (Critical Infrastructure Protection) expertise to multiple industry sectors. They have had a broad perspective on working with various entities in the Oil and Gas, Independent Power Producers, integrated utilities, municipalities, cooperatives, and transmission companies across all NERC regions. <u>STROBES: Strokes Security Inc.</u> is the market leader in the vulnerability management space. The team developed and refined the process for vulnerability management, transforming it into an Enterprise-grade solution for all organizations. The solution seamlessly and effectively identifies vulnerabilities and follows a validated process to efficiently resolve the findings. Strokes coordinates activities for those involved in threat management, equips them with innovative technology. conduct customized tests based on technology and business logic; the entire pen test will be carried out by our skilled and certified security engineers. Our senior penetration testing engineer will perform a detailed risk assessment on the vulnerabilities found, carefully weed out false positives and assign a scoring system based on CVSS (Common Vulnerability Scoring System) on to the findings. <b>Project 1: Veolia North America</b> cybersecurity self-assessment of Veolia's OT (Operational Technology) facilities for evaluation of their current Operational Technology (OT) security posture against ISA/IEC 62443 and provided recommendations designed to help manage cybersecurity risks, Penetration Testing, Source Code Review and Red Team Assessment. <b>Project 2: California based financial services company:</b> Quarterly Penetration Test for - Web Applications - 16 Nos- Mobile Application (android & iOS) - 10- Thick Client Applications - 5• Source code reviews- Once a year - 19 web applications, 8 mobile apps• Red Team Assessment once a year Key Outcomes• Identified 2000 critical and high severity vulnerabilities in a year.• Improved the security posture of web and mobile applications.• Helped to mitigate all the issues in a timely manner.• Supported the client in achieving multiple compliance audit <b>Project 3 A Software Development company:</b> Performed Penetration Test for • Web Applications - 45 Nos• Mobile Application (android & iOS) - 68• Source code reviews- 20 critical web applications, 40 mobile apps• Internal and External Network Penetration Testing- 40 Subnets• Performed segmentation testing as per PCI guidelines. Key Outcomes• Identified and reported 200+ security issues and 100+ misconfigurations.• Improved the security posture of their cloud infrastructure through config review and pen test solution.• Improved their vulnerability management program by introducing our VM platform and helped them mitigate all the reported issues in a timely manner.• Helped them achieve meet PCI guidelines. (Project 2 and3 are one year) <b>Project 4: Oil and Gas Organization:</b> internal and external penetration testing assessment for a \$1 billion oil and gas energy client, Itegriti assessed cybersecurity capabilities, emphasizing risk mitigation for OT/IT network convergence, and determining the extent to which relevant security controls were appropriately designed, implemented, and effective. The production environment for this testing included two supervisory control and data acquisition (SCADA) systems using "pull" technology. Wireless devices with I.P. filtering collected data from older sites and transmitted it to a local on-premises SCADA system synchronized with corporate offices via a wide area network (WAN) link). Data from newer sites leveraged a more modern cloud-based SCADA system with centralized dashboards and monitoring. <b>Project 5: Leading Semiconductor Company,</b> providing Application & Infrastructure Vulnerability Management and Remediation Support services to a leading semiconductor company that serves various markets, such as data center, networking, software, broadband, wireless, storage, and industrial. The company is headquartered in San Jose, Californian <b>Project 6: Municipal Utility, providing reliable power and water to 1.4M,</b> penetration testing and security assessment for their Generation Management System (GMS). The engagement also included providing a security assessment of remote access methods used for the GMS, Energy Management System (EMS), and Supervisory Control and Data Acquisition (SCADA).The cybersecurity evaluation included the following:• Installation of virtual machines and penetration testing tools on the client-provided laptop• Review of client-provided network documentation, system configuration information, and cybersecurity-related procedures for accessing the GMS, EMS, and SCADA environments• Validation of specified IP addresses to be tested based on information supplied by the client.• Performing Black Box Testing attempting to access network devices in the GMS environment remotely via an Internet connection• Conducting White Box Testing using a client-provided network IP connection within the electronic access and control system DMZ. (overall - for the two project that included a timeline seemed long. Projects are large and complex and reflect the type of work we noted in the RFQQ. Not extensive experience with state local governments)
Staffing (30%)	30.0	25.0	<u>1_ Sivakumary director threat and vulnerability management:</u> 20 years IT background, certifications include CEH, has technical skills related to penetration testing applications. <u>2_ Victor senior penetration tester ethical hacker and trainer:</u> background in network, wireless, web application penetration testing, vulnerability research, exploit development networking security over 21 years developed and documented ethical hacking web application hacking exploit development protocol fuzzing and vulnerability research training sessions using Metasploit framework. extensive certifications, <u>3_ Bhargav, senior consultant:</u> 10 years in IT security experience including security, vulnerability assessments, red teaming Wi-Fi security assessment, experience well defined and good certifications related to penetration testing. <u>4_ Pavan Kumar Mallem:</u> 5 years experience in vulnerability assessment and penetration testing of networks, web applications, API, and mobile apps including red teaming. reported bug to Sony, Adobe and SMTPsGeotc. <u>4_ Shiva:</u> 7 years experience in web and mobile app VAPT, network spear phishing red team and code review. Several bug bounty's reported - flipkart, urban, Oppo, Zomato, AT&Tm Sony and general motors and US DOD, hall of fame in pytm in 2018. <u>5_ Prakash, Sr. Security Analyst:</u> seven years experience in IT managed security assessments for government and other sectors. Experience in web mobile and VAPT source code network and red team and has penetration testing related certifications. (overall - 5 key staff all with penetration testing, bug bounties good not a lot of experience with state and local government but depth of penetration testing experience)
Qualifications Section Total Score	65.0	57.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	12.0	Targets included - provided sample reports for different scopes. The content and remediation steps are clear <b>yes</b> . Separate sections for management and technical audiences; <b>yes the second and third reports but very technical</b>  An executive summary that presents findings, conclusions and recommendations; .No Ingeriti <b>Yes Inspira, findings not recommendations, the third report has recommendation in the ES</b>  Testing methodology and a description of procedures used - testing methodologies should be described at a level of detail so that they are re-creatable using screen prints as necessary; Indpits has a testing methodology, <b>no testing methodology, screen prints in findings yes</b>  All test results and findings, including identification of tests performed that did not identify issues; <b>Yes all test results no to tests that did not identify issues</b>  Ranked results with a standard rating scale (likelihood and significance) detailing the seriousness of each finding and remediation prioritization; <b>YES</b>  Detailed information about how each issue can be fixed and the level of effort to fix; <b>Yes but no to level of effort but it was provided in later reports</b> A description of the implications or impact of not fixing each of the issues noted; <b>Yes</b>  An overall assessment based on the work performed for each agency and/or government including strengths and opportunities for improvement. <b>No</b>
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	69.0	
Date:			
working with integrity and strobes			

K689 - Security Assessment Services			
Vendor: KPMG			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit. 360 hours approach was not included
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	28.0	has build several methodologies for API testing, threat modeling and full stack security assessments. On average pen testers have between four and seven years of experience with senior leaders have over 10 years of offensive security experience or hundreds of tests across all domains of penetration testing to deliver outstanding outcomes to our clients that holistically improve their security postures from a full stack perspective. <b>Project 1 US FISMA Audit Support to DOE:</b> Penetration testing of the agencies FISMA reportable systems and applications in support of their annual FISMA reporting Internal and external penetration testing, individual field office and laboratories. project takes 5 months and is done annually. Identify 50,000 to 100,000 vulnerabilities per year on average. <b>Project 2: Global Financial Services Firm,</b> managed automated vulnerability discovery and penetration testing for manual web application testing, automated web application testing, automated and manual source code review mobile application penetration testing, remediation verifications and assessment coordinators to test and identify vulnerabilities in thousands of applications and change requests per year. 1 year <b>Project 3: Industrial Automotive Manufacturing Company:</b> penetration test of the corporate internal network and external penetration testing. 750 IPS on two separate network. External testing on 50 IPS included root cause analysis, three months <b>project 4: Utilities company:</b> identify vulnerabilities within their IT environment across their worldwide network. three months. Focused on gaining unauthorized access to the corporate enterprise sensitive data and protected areas of the SCADA environment. Trend Team exercises included internal penetration testing, external penetration testing, web application testing social engineering, three months <b>Project 5 US Homes Manufacture</b> external threats to their production web site and perimeter assets and in an assumed breach scenario. internal penetration testing of thousands of assets, goal focused on elevated domain enterprise admin privileges accessing sensitive systems aor assets and accessing confidential or sensitive information. external penetration testing for hundreds of assets including a vulnerability assessment and false positive analysis. web application penetration testing for production and development web application in both unauthenticated and authenticated roles leveraging automated scans to perform manual penetration techniques and false positive analysis. 3 months (overall Project three: did not full redact on page 64, all projects include penetration testing including SCADA do not see thick client timing looks reasonable)
Staffing (30%)	30.0	15.0	1. Rahul Kohi, Principal.21 years of experience in cybersecurity an privacy assistance to State and local. Medicaid. reduce risk of cybercrime and compliance. Led a penetration testing project for an industrial manufacturing client lead or delivery manager for several IT security projects. Not a penetration tester 2. Daniel Engagement Advisor Federal Advisory practice with strong knowledge in cyber security testing. focus on security testing, security controls assessments, IT audit reviews and technical controls testing including penetration testing and vulnerability assessments. performed penetration testing both externally and internally over high value systems with FISMA high and medium designations. CEH 3. Evan engagement advisor managed application security testing practice with 15 year experience performed testing services on numerous engagements, managed testing and compliance teams application and network testing services, cybersecurity audits, governance, risk and compliance. external and internal penetration testing, web app and API testing, CISSP. 4. Tarun Sondhi, Principal and delivery lead: 20 years experience he specializes in designing and deploying innovative solutions to protect enterprise systems. Architected and led development of advance analytics modules to detect unknown cyber activities at industrial Manau acting organization with SCADA and ICS. Not a penetration tester but IT security professional. 5. Engagement Manager, Specialist Director 20 years experience in technology cybersecurity and business. CISSP not a penetration tester. 6. Griffin Reid, Technical manager. performing network and web application penetration tests. 14 years of experience including network and application security, red team engagements wireless security testing physical security testing and system configuration and hardening reviews. code analysis, software composition analysis architectural design review and threat modeling, CISSP, CISA GWAPT 7.Christopher Day security testing SMP, 12 years in cybersecurity, led the penetration testing portions of over ten proposals for federal clients; performed external web application penetration for over 35 publicly facing web applications; lead over 100 vulnerability and compliance audit events. 8. Weston H Cole, Lead Specialist, security testing SMP, six years of cybersecurity, lead network penetration testing engagements conducted by both internal and external testers. CISSP. (overall of eight staff, three are penetration testers one of the engagement advisors was a tester; heavy oversight from cybersecurity specialists that do not specialize in penetration testing. unclear if three testers have experience testing all types of penetration testing in the RFQQ including SCADA and thick client)
Qualifications Section Total Score	65.0	43.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	12.0	<b>Targets included internal network assessment and web application assessment</b> . The content and remediation steps are clear . Separate sections for management and technical audiences; <b>Yes but technical,</b>  An executive summary that presents findings, conclusions and recommendations; <b>YES.</b>  Testing methodology and a description of procedures used - testing methodologies should be described at a level of detail so that they are re-creatable using screen prints as necessary; <b>Yes</b>  All test results and findings, including identification of tests performed that did not identify issues; <b>Yes but not tests without results</b>  Ranked results with a standard rating scale (likelihood and significance) detailing the seriousness of each finding and remediation prioritization; <b>Yes</b>  Detailed information about how each issue can be fixed and the level of effort to fix; <b>YEs not level of effort</b> A description of the implications or impact of not fixing each of the issues noted; <b>Yes</b>  An overall assessment based on the work performed for each agency and/or government including strengths and opportunities for improvement. <b>YES</b>
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	55.0	
Evaluator Initials :			
Date:			



K689 - Security Assessment Services			
Vendor: Lumen			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit. 524 hours. In the approach note inclusion of OSINT in the information gathering phase. A good amount of information provided to understand the methodology and approach for each type of testing included in the example - external internal mainframe firewall config etc. Two months for this project. Gave timeframe of 30 months for all entities under audit. shows they can do two audits at a time. Good plan and breakout of tasks with timeline.
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	20.0	provided these services to 100s of Federal, State and Local Agencies and Governments and Commercial Clients provided these services to 100s of Federal, State and Local Agencies and Governments and Commercial Clients. assessments cover:Web applications: Identifying common web application vulnerabilities, such as SQL injection, cross-site scripting (XSS), and authentication flaws. Thick client applications: Analyzing desktop applications for potential security issues, such as insecure data storage, weak encryption, and privilege escalation vulnerabilities. Mainframes: Assessing mainframe security configurations, access controls, and potential vulnerabilities in legacy systems. Operational technology: Evaluating the security posture of industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) systems, and other OT components. Network: Examining network infrastructure for misconfigurations, weak encryption, and other vulnerabilities that could lead to authorized access or data breaches. Source code: Reviewing application source code to identify potential security flaws. <b>Project 1:</b> external and internal network testing, web application testing, and Wi-Fi penetration testing. <b>Project 2 Ethos Group</b> conducted an engagement with an energy sector organization resulted in the discovery of default credentials on a web server, which if exploited could have provided an attacker with easy access to make unauthorized changes. Our team of experts utilized cutting-edge tools and techniques to identify and exploit vulnerabilities, enabling us to provide actionable recommendations to remediate security weaknesses. In addition to discovering the default credentials, our report included recommendations to improve credential management to prevent similar incidents in the future. <b>Project 3: Center for Dialysis care</b> ; performed a security penetration test which included the following aspects: OSINT, external networks, internal networks, web applications and Wi-Fi. During the course of the testing, Lumen uncovered critical and high vulnerabilities in virtually all testing areas. Even though vulnerabilities and weak encryption were pervasive throughout the organization, the biggest vulnerability was through configuration of their directory. It was accepted policy that they shared the administrator account and password with dozens of help desk and IT employees (confidential information included in the sample projects) <b>Project 4: Penske Media Corporation:</b> penetration test for Penske Media Corporation, which included the following aspects: OSINT, external network (15 targets), and internal network (600 targets) attacks. During testing, Lumen uncovered a number of moderate security risks, including a successful compromise of network attached storage which led to the disclosure of sensitive information. <b>Project 5: CU Direct</b> a security penetration test for CU Direct, which included internal network attacks (3500 targets). During testing, Lumen uncovered a number of moderate security risks, including a successful compromise of Windows operating systems which allowed command line access(Overall, good examples of penetration testing, not clear they covered all the testing noted in the RFQQ all examples were private companies not government, <b>confidential information included in the sample projects</b> )
Staffing (30%)	30.0	25.0	<b>1. Mike Ramer</b> , Senior Manager of Security and risk consulting, CISSP, Perform security assessments of transmission control systems (ICS/ICT, IT security professional <b>not a penetration tester</b> . <b>2. Tom Fulton</b> security penetration tester: lots of certifications, Wi fi, web applications internal and external network, develops penetration testing procedures and runbooks. <b>3 Keon Morrison security penetration tester</b> , lots of good credentials completed several Internal, External & Wireless AP Penetration Test for high value clients.♦ Updated Methodologies and Penetration Testing procedures.♦ Proposed, designed, and advocated for Customer Portal creation Following the MITRE Attack framework, I perform manual Application & Perimeter Network infiltration testing (Red Team) for Optum assets. Using all possible tools, I discover & exploit security flaws involving all the OWASP Top 10 and CWE 25 vulnerabilities. I use extended Nessus, Burp Suite Pro, much of the Kali Linux toolset, Metasploit, google searches & Stack Exchange. I support dev teams with completing DevOps requirements and previously performed as Product owner/Admin for SecOps tools such as Rapid7 & Whitehat.♦ I act as security SME and aide the Enterprise vulnerability Management apparatus. Highlights include:♦ Compromise of numerous HealthCare & Payment applications leveraging exploit chains that included: enumeration, programmatic fuzzing, vuln discovery & custom Python exploit development remote payload delivery & remote code execution (RCE). ♦ Private disclosure of critical severities of OWASP Top ten & CWE 25 vulnerabilities for Mobile Apps, API, Web and Cloud. Red team. authored the Blackbox Penetration Testing guide used by the Ethical Hacking Team performed manual and automated security testing against financial applications.♦ I reverse engineered software using OllyDBG and IDA-Pro and conducted source code review. <b>4. Nick Hutchison penetration tester</b> , lots of good credentials, g internal, external, and web application tests, wireless healthcare, private industry <b>5. Erik Rives, Lead security consultant CISSP</b> g internal, external, and web application tests. documentation, incident response during penetration testing, reporting. (overall, three very experienced penetration testers, one manager and one lead, Keon is very impressive experience and accolades. )
Qualifications Section Total Score	65.0	45.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	14.0	<b>Targets included internal external web applications.</b> The content and remediation steps are clear <b>yes</b> . Separate sections for management and technical audiences; <b>Yes clear to both audiences</b>  An executive summary that presents findings, conclusions and recommendations; <b>.Yes</b>  Testing methodology and a description of procedures used - testing methodologies should be described at a level of detail so that they are re-creatable using screen prints as necessary; <b>Yes</b>  All test results and findings, including identification of tests performed that did not identify issues; <b>Yes</b>  Ranked results with a standard rating scale (likelihood and significance) detailing the seriousness of each finding and remediation prioritization; <b>Yes</b>  Detailed information about how each issue can be fixed and the level of effort to fix; <b>Yes not level of effort</b> A description of the implications or impact of not fixing each of the issues noted; <b>yes (e.g. able to exploit a vulnerability but not pivot)</b>  An overall assessment based on the work performed for each agency and/or government including strengths and opportunities for improvement. <b>Yes</b>
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	59.0	
Evaluator Initials :			
Date:			



Online			
K689 - Security Assessment Services			
Vendor: Online			
Quotations Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit. 276 hours. Great breakdown by penetration testing task and hours look good. Seven weeks from scoping to draft report, looks good timeline. Good methodology and approach detailed for each type of testing included in the sample agency except SCADA just notes this has been done with no downtime and notes some good risk management techniques and importance of communication. Nothing separate noted for thick clients just web applications.
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	28.0	contracted with both public and private organizations to conduct monthly assessments through a subscription-based model and provide ongoing insights into vulnerabilities within their environments. experienced with a diverse range of industry leading tools. We pride ourselves in our ability to root out false positives and work with our clients to transfer knowledge to help the organization evolve their security programs experience across an array of environments including internal and external networks, wireless networks, applications, application programming interfaces (APIs), mobile apps, and cloud environments. Specific to the public sector, we have conducted internal and external penetration testing, SCADA, and OT testing for multiple statewide agencies ranging from healthcare, workforce services, and municipalities. We have a proven track record of successfully exploiting discovered vulnerabilities in both test and production environments containing highly sensitive information or mission critical systems requiring high availability. <b>1. Wyoming Department of Health:</b> vulnerability assessment, internal network penetration testing, application penetration testing, security controls review, and provide security expertise and testing throughout the implementation and integration of modules. 4 years but not clear how long the penetration services took. <b>2. Statewide workers compensation insurance provider:</b> External and Internal Penetration Testing for a statewide Workers Compensation Insurance Provider as part of their PCI Compliance, one year. <b>3. Louisiana local city government agency.</b> external and internal network penetration testing four weeks. <b>4. National health information network.</b> external and internal penetration test network, 5 weeks. <b>5. Community college commission;</b> internal and external timeline is 2019 to current so unclear on timeline for testing ( all project include penetration testing with local governments, projects have a narrow scope and not clearly demonstrating examples of the scope of work in the RFQQ including thick clients and Scada, timeline looks long for small scopes like 4 weeks for network internal and external but if includes reporting then it would be good timing)
Staffing (30%)	30.0	25.0	<b>1. Will Bechtel,</b> Penetration tester CISSP, Expert in designing and executing automated vulnerability assessment tools including dynamic analysis tools for network and application testing, as well as secure code analysis tools that evaluate source code. Government and utility experience. Will has deep experience integrating various security products via APIs. security assessments and penetration testing. <b>2. Warren Campbell, penetration tester</b> 8 years experience CISSP OSCP OSWP Principal Security Consultant, Wireless penetration testing - encryption and authentication Assessment included evaluation of authentication protocols, cracking of WPA2 PSK handshakes, and man-in-the-middle of WPA2 Enterprise networks , infrastructure penetration testing web application testing. Network penetration testing - thousand hosts within the internal network. Machines included end-user workstations, Windows and Linux Server, Firewalls, Load Balancers, and Credit Card processors. Infrastructure penetration tester of jail water treatment plant, small government, healthcare, energy. Michael Sringer, technical expertly red team vulnerability assessments <b>3. Michael Stringer, penetration tester</b> specializing in attack and defense, ethical hacking, and penetration testing with over 8 years of experience in the IT field. Penetration testing, wireless network, application testing, oil and gas, retail healthcare. <b>4. David Bulloch, penetration tester Senior Analyst/Consultant</b> GWAPT GPEN, with significant experience in application development and application integration projects manage, plan, execute, and provide detailed reports on security vulnerability assessments - including network and application penetration tests used to identify security weaknesses in targeted environments. excellent application development skills. proficient in a wide variety of development tools, with specific expertise in Java, Sonic, Oracle, PowerBuilder, and Versata. fulfilled the role of technical mentor and coach in these different environments. has worked on numerous penetration testing and vulnerability assessment engagements, with emphasis on web application and network testing (internal and external). 5 years experience with penetration testing telecommunications, insurance, retail, transportation, government, along with fortune 500 corporations. Penetration testing engagements range from net-new assessments to annual compliance checks, testing duration ranges from a few days to a few weeks lots significant of local and state government experience including WA <b>5. Jason Nguyen penetration tester</b> GPEN, GWAPT, GCIH, 10 years experience in IT security application security vulnerability management and penetration testing. red team and blue team experience. <b>6. Melissa Erikson Project Manager</b> a project leader with over 18 years' experience in public and private healthcare. Her diverse portfolio includes overseeing state and federal government IT certification and security projects, managing the implementation of IT systems, and supporting clients through policy and governance development. Melissa has supported state agencies across the U.S. including Wyoming, Colorado, Oregon, Minnesota, Iowa, and Montana.; <b>7. Rob Harvey Oversight and Governance</b> Managing Director of Online Business Systems' Risk, Security and Privacy Practice security consulting experience and over sixteen years in Information Technology; <b>8 Mark Van Patten, Delivery Oversight and escalation</b> 25+ years of consulting experience and managing the delivery of IT services (overall government experience extensive with some staff, 5 have penetration testing experience and good certifications; 3 staff doing project manager, oversight and direction)
Qualifications Section Total Score	65.0	53.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	12.0	<b>Targets included web application, four days.</b> The content and remediation steps are clear <b>YEs.</b> Separate sections for management and technical audiences; <b>Yes but it is on the technical side</b>  An executive summary that presents findings, conclusions and recommendations; <b>Yes</b> .  Testing methodology and a description of procedures used - testing methodologies should be described at a level of detail so that they are re-creatable using screen prints as necessary; <b>Yes</b>  All test results and findings, including identification of tests performed that did not identify issues; <b>Yes not tests that did not identify findings</b>  Ranked results with a standard rating scale (likelihood and significance) detailing the seriousness of each finding and remediation prioritization; <b>Yes</b>  Detailed information about how each issue can be fixed and the level of effort to fix; <b>Yes not the level of effort to fix</b> A description of the implications or impact of not fixing each of the issues noted; <b>Yes good description of issue if not fixed</b>  An overall assessment based on the work performed for each agency and/or government including strengths and opportunities for improvement. <b>Yes</b>
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	65.0	
Evaluator Initials :			
Date:			



K689 - Security Assessment Services			
Vendor: Peraton			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit. 333 hours to complete. five weeks to draft report from project kickoff is a good timeline. Good detailed methodology for the different testing targets noted in the sample agency. nothing specific for thick client jut noting web technologies typically dominate.
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	32.0	For over 20 years Peraton Labs has performed security assessments for large enterprises, utilities, telecom carriers, healthcare providers, banking institutions, major movie studios, and government agencies. <b>Project 1 Ohio Bureau of Workers' Compensation (BWC) Security Testing.</b> IT security and vulnerability assessment and penetration test of a state's workers compensation agency, provider of workers' compensation insurance in Ohio, serving 257,000 public and private employers. With nearly 1,600 employees and assets of approximately \$21 billion, one of the largest state-run insurance systems in the United States. Areas assessed included Internet facing infrastructure including multiple web application sites, VPN Connectivity, and file transfer; employee and guest Wi-Fi access; internal network attacks; social engineering, including phishing and USB device drops; and user laptop configuration resilience against malware and privilege escalation. The Internet facing areas assessed were VPN connectivity; current Production and Performance Test websites; externally facing SharePoint; Web Chat; authenticated testing of externally facing Web Services; and external file transfer site. <b>Project 2 Sacramento Municipal Utility District.</b> a vulnerability assessment and penetration test of a West Coast Municipal Utility's Internet-facing infrastructure and web application security assessment. <b>Protect 3 Exelon 500 G/W Security Assessment 2021 – 2022</b> evaluate the security risks and vulnerabilities with overlaying an Advanced Metering Infrastructure (AMI) for gas and water meters on its electric Smart Grid field network as part of a new Network-as-a-Service business model. Management application software security (web application) and architecture review, network security and wireless communications security (active and passive) <b>Project 4 Entergy Assessment of New Supply Chain and Asset Management System.</b> 7 months: Peraton Labs conducted a security assessment against Entergy's new MaxGen Supply Chain and Asset Management System before the system went live. This system is a highly integrated, virtualized and containerized operations system that interfaces with numerous applications across Entergy's infrastructure. The assessment was split across a number of tasks:• Core Platform Architecture and Threat Analysis• Deep dive assessment of Kubernetes systems, including DevSecOps and CI/CD• Assessments of multiple Vendor Software Products including Middleware solutions• Assessments of select interfaces and integrations with other Entergy systems• Network and host assessments of relevant systems• Review of New Segregation of Duty features in Entergy's Identity Management Solution• Assessment of Monitoring, Logging, Alerting and Reporting capabilities. <b>Project 5 Iconectiv Vulnerability Assessment / Penetration Test.</b> annual vulnerability assessment and penetration test for iconectiv on two Internet-facing applications one is serverless internet facing with third party industry systems one is on premise web application. Serverless - an assessment of the SCR application, its APIs, and the server supporting file transfers. Prior versions of the application were implemented using on premise servers. With the move to AWS serverless platform Peraton Labs focused on the architectural areas where the rewrite and changed integrations could lead to security weaknesses. This included conducting a limited source code review and identification of insecure programming practices, focused on the new AWS Lambda TypeScript back-end functions. API configuration. (All five examples are thorough penetration tests as detailed in the exhibit, two include state government. Highly technical penetration tests including thorough consideration of architecture and unconnected systems complex cloud based systems. some concern over 7 month time frame for project 4. Sounds like they assisted the clients in understanding their environments, risks, and helped make improvements and tested so timeline extended. )
Staffing (30%)	30.0	28.0	application security, cloud security (including AWS), and network security. web application and network penetration testing for large, complex applications and environments. He is well versed in multiple control frameworks, including NIST 800-53, PCI-DSS, HIPAA and NERC CIP. He has provided support for a wide range of federal, state, and local agencies, including the FDA, FRB, Treasury Bureau of Fiscal Services, US Postal Service, DISA, State of Florida, Ohio Department of Taxation, City of Irvine, and others. He has also support multiple clients in the energy sector, including Entergy, Exelon and others. FedRAMP assessments. Responsibilities included all aspects of engagement management, including SOW/Proposal development, performing assessments, project management, customer communications and final review of all deliverables. Complex OT and cloud assessments. Lot of utility and government experience. <b>2. Janine Security+, GSEC, GCIH, GPEN.</b> security researcher and penetration tester with certifications and experience in Information Security. Previous experience in Enterprise Systems Administration and Web/Software Development in education & local government industries. US Cyber Challenge Top Scorer, Center for Internet Security. Three yeas as a tester network and web application and vulnerability assessments. wireless traffic monitoring. IT experience14 years. <b>3. Michael CISSP</b> Cyber security expert specializing in vulnerability analysis and penetration testing with over 15 years providing cyber security professional services. Perform hardware, application, wireless and network technical security assessments and penetration testing focusing on Smart Grid, SCADA and industrial control systems Perform protocol reverse engineering to discover inherent security vulnerabilities as well as vulnerabilities introduced in specific implementations.□ Develop proof of concept exploits for discovered vulnerabilities.□ Develop custom protocol layers in Python for testing devices with proprietary networking stacks. Prepared and delivered technical briefings and presentations to division technical directors, NSA senior leadership, military leadership, Government second parties and other IC members.□ Developed specialized network forensic tools for Blue Team usage. <b>4. Stephen McNaught, PMP, CISSP:</b> Principal Cyber Security Consultant in Peraton Labs with over 30 years of security experience in carrier grade networks and cybersecurity research, Stephen has an extensive work history covering diverse technology and security disciplines with government, utilities, commercial and non-profit domestic and international customers. He has performed security research, analysis and published on risks, vulnerabilities and assessment methodologies for Applications, Network Infrastructure, Smartphone, Industrial Control Systems, IPTV, Intelligent Transportation Systems, Smart Grid and Cloud technologies. Wrote an Intelligent Transportation Systems (ITS) Penetration Testing Concepts document for the U.S. Department of Transportation. The document was utilized in the development of a standardized ITS penetration testing methodology published to the industry which was co-authored by Stephen. As part of the DOT project, Stephen lead the penetration testing of the ITS environment for the County of San Diego that included applications, networks, wireless systems, and embedded field controllers. The penetration test included the testing of the DOT production ITS, Metropolitan Area Network (MAN), Secure DMZ and Corporate networks. ITS components under test included curbside traffic signal control systems software and hardware, messaging systems, streetlight controls, video detection systems and security monitoring applications. technical lead for multiple security assessments that involved physical, network analysis and penetration testing of a Fortune 500 integrated energy company engaged primarily in electric power production and retail distribution operations ( <i>capacity-three projects in experience are ongoing</i> ) Performed network packet capture analysis to reverse engineer proprietary protocols to identify security weaknesses for a major commercial client. <b>5. Marcus: CISSP,</b> about ten years as a penetration tester. Areas of Expertise: cyber-security, software development, networking, simulation, automotive telematics. Performed security assessment and penetration testing for networks and web servers for multiple clients. Extensive experience performing application security assessments and penetration testing for commercial businesses, utilities and government agencies. research and innovation- 1998-2012. <b>6. Josiah Keller, Software Engineer 4 years.</b> Software developer and reverse-engineer with experience spanning the high-level to the low-level.• Ghidra (incl. scripting) and IDA Pro• x86, x64, 68000, and ARM• C, Python, JavaScript, other programming languages• Full-stack web development Reverse-engineering device firmware with Ghidra• Writing Ghidra scripts to automate analysis• Improving internal debugging tools• Re-hosting firmware under emulation• Developing tools for assessing control device integrity. <b>7. Jason Youzwak,</b> Over 25 years of experience in software development life cycle, including requirements reviews, system architecture, object-oriented design, development, testing, installation and deployment□ In-depth experience with Smart Grid field area network security and management systems. Developed SecureSmart tools for network monitoring and analysis and intrusion detection in AMI, DA and SCADA networks. Performed in-depth AMI/DA/SCADA security assessments for major utilities□ Broad experience in identifying and exploiting vulnerabilities on a variety of platforms including web applications, client/server applications, IP networks, and multi-media platforms□ Performed source code analysis to identify vulnerable code using various analysis tools and reverse engineering to identify Smart Grid proprietary messaging□ Extensive background on UNIX including installation of operating systems, creating build procedures, automating tasks, and troubleshooting performance problems. security research and vulnerability testing- network web and database. 13 publications in cybersecurity. (All 7 key staff have testing experience with some having exceptional technical and cybersecurity backgrounds. depth of experience is exceptional; two staff have less experience with testing more experience with IT Janine Josiah)
Qualifications Section Total Score	65.0	60.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item “d.” under “Report Results” on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	13.0	<b>Targets included security architecture and configuration review, external network scan and vulnerability assessment, internal network scan and assessment, external web application security and vulnerability testing review of AWS private cloud architecture and settings.</b> . The content and remediation steps are clear <b>YES.</b> Separate sections for management and technical audiences; <b>Some summary information but highly technical</b>  An executive summary that presents findings, conclusions and recommendations; <b>yes also included management and governance identity and access management recommendations and a review of best practices that were no security but overall implementation success for AWS .</b>  Testing methodology and a description of procedures used - testing methodologies should be described at a level of detail so that they are re-creatable using screen prints as necessary; <b>YES</b>  All test results and findings, including identification of tests performed that did not identify issues; <b>YES, good account of information on tests performed and their purpose</b>  Ranked results with a standard rating scale (likelihood and significance) detailing the seriousness of each finding and remediation prioritization; <b>Yes</b>  Detailed information about how each issue can be fixed and the level of effort to fix; <b>yes but not level of effort to fix</b> A description of the implications or impact of not fixing each of the issues noted; <b>yes</b>  An overall assessment based on the work performed for each agency and/or government including strengths and opportunities for improvement. <b>Yes but not strengths</b>
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	73.0	
Evaluator Initials :			
Date:			



PlanteMoran			
K689 - Security Assessment Services			
Vendor: Plante Moran			
Quotations Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit. 334 hours. Overview of methodology provided.
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	21.0	Our penetration testing follows industry-standard approaches, including CREST, PTES, ISSAF, MITRE, NIST, and OWASP. certified public accounting and management consulting firm. 500 government clients. e extensive experience in the assessment of cybersecurity controls, IT policies and procedures, IT compliance laws and regulations, and IT infrastructure and tools used to support the business that will lead to the development of a clear vision for the future environment. Within the 30 years of providing cybersecurity and consulting services, we have supported and performed over 500 security engagements. cyber professionals have, on average, more than 13 years of experience performing cybersecurity control evaluations, IT compliance testing, internal audit assistance, technical assessments, and internal control consulting services. CEH, GIAC GPEN, Security, Network TIA+, CISSPeCPPT. <b>Project 1 Ohio Public employees retirement system.</b> 3 weeks external network penetration testing, external network vulnerability assessment, web application security assessment, and wireless penetration testing to identify vulnerabilities and recommend appropriate safeguards to enhance OPERS's overall security controls. <b>Project 2 The Joint Commission</b> External and internal network penetration testing• Network vulnerability assessment• Web application security assessment. <b>Project three Ohio Deferred Compensation</b> •6 weeks external and internal network penetration testing, quarterly network vulnerability scanning, web application security assessment, and source code review of their participant portal to identify vulnerabilities and recommend appropriate safeguards to enhance Ohio Deferred Compensation's (Ohio DC's) overall security controls. <b>Project 4. City of Tacoma WA.</b> 2.5 months External PCI network security penetration testing• Internal PCI network security penetration testing• Network vulnerability assessment (external and internal)• Segmentation testing and PCI scope validation. Project 5: Outfront media, 6-8 weeks annually, external and internal network penetration testing, web application security testing, and an Amazon Web Services (AWS) Identity and Access Management controls (all projects include penetration testing but not clearly aligned with RFQQ including OT SCADA or thick client)
Staffing (30%)	30.0	15.0	<b>1. Mike, Partner, Engagement partner, serve</b> as the primary point of contact and will have the overall responsibility for engagement account management. Responsible for ensuring that all Plante Moran services are completed within schedule and budget. Will provide project quality control over Plante Moran deliverables and services Mike has spent 32 years in information technology, 20 plus of those focused on information security and risk. Mike has hands on experience building, managing and maturing IT, information security, risk, governance, business continuity, and privacy programs in his roles as CIO, CTO, and CISO; Mike has also worked closely with both the energy sector and government on protecting critical infrastructure. <b>Alex, Project Manager overall project management,</b> team management and day to day communications. Responsible for risk and issue management and regular project communications with the management team and SAO. 25 years of information technology audit, technology regulatory control compliance, and system integration project experience <b>3. Saumil, CEH CISSP, Penetration testing lead.</b> 17 years of information security, control, and IT audit experience in a number of industries, including financial institutions, insurance, and healthcare. Samuel's experience includes reviewing system configuration (router/switch/firewall/server settings etc.), conducting web and mobile application security, source code reviews, and social engineering assessments, as well as performing black-box/white-box network penetration testing on IT infrastructure components deployed and managed by the client infrastructure team <b>DeShaun, OSCP;</b> experience in education, financial industries, manufacturing, and the service industry, as well as assisting clients with configuring their SIEM solution. Within Plante Moran's cybersecurity practice, DeShaun's area of focus is on penetration testing, vulnerability assessments, and social engineering <b>Trent, OSCP GPEN GWAPT</b> experience with multiple technologies, ranging from server administration to telecom and network engineering, <b>Shayna</b> 10 years of experience in various aspects of Information Technology ranging from hardware, software, networks, and administration to security, <b>Michael,</b> worked in a network operations center at an internet service provider, gaining experience in tackling many of the networking and security issues that businesses face. <b>Parth CEH, ECSA, SNSS, CSCU, CISC, CPFA.</b> an experienced cybersecurity professional with expertise into performing advance penetration testing and cloud security assessment. His work encompasses several industries including healthcare, financial technology, media and entertainment, manufacturing, and IT. Parth's experience includes internal and external penetration testing, web application security, vulnerability assessment, and social engineering assessment and Anas network security professional with experience in antivirus and host based intrusion prevention, spear phishing attack prevention using DMARC, and Zscaler deployment. He performs vulnerability assessments and has years of experience working with drive encryption, have each participated in numerous Penetration Assessments as listed in our reference section. They bring hands-on experience from 1-5 years with assessing technical networks, performing penetration vulnerability assessments, and evaluating people, process and technologies associated with risk management and developing recommendations. (six testers with 1-5 years experience ; Alex and Mike has IT experience but not penetration testing need to ensure depth or review given 1-5 years is not significant experience but some experience experience).
Qualifications Section Total Score	65.0	36.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	12.0	<b>Targets included external network security and penetration , social engineering, internal network security and penetration testing and network vulnerability assessment.</b> The content and remediation steps are clear <b>yes.</b> Separate sections for management and technical audiences; <b>Yes good management section</b>  An executive summary that presents findings, conclusions and recommendations; <b>Yes.</b>  Testing methodology and a description of procedures used - testing methodologies should be described at a level of detail so that they are re-creatable using screen prints as necessary; <b>Yes, what we did</b>  All test results and findings, including identification of tests performed that did not identify issues; <b>Yes</b>  Ranked results with a standard rating scale (likelihood and significance) detailing the seriousness of each finding and remediation prioritization; <b>yes</b>  Detailed information about how each issue can be fixed and the level of effort to fix; <b>not level of effort but yes to detailed information on how to fix. Also good information on general policy recommendations tied to specific conditions</b> A description of the implications or impact of not fixing each of the issues noted; <b>Yes to most</b>  <b>An overall assessment based on the work performed for each agency and/or government including strengths and opportunities for improvement. YES good security scorecard giving overall assessment and strengths noted</b>
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	48.0	
Evaluator Initials :			
Date:			
written as an assessment of SAO			



K689 - Security Assessment Services			
Vendor: RSI			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit. 462 hours. Methodology for each section of the testing is detailed out. Noting manual and automated processes that use commercial, open source, and proprietary software will be used for testing. Includes remediation testing. Timeline seems okay but its it all done at the same time or one after the other? external testing 10 days, internal 6 days, OT 25 days, firewall 2 days, web app 6days mobile app 4 days, thick client 4 days, (what does findings published in Resolve at engagement conclusion mean? and access to findings in resolve for one year mean?)
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	21.0	1. <b>Telecom corp.</b> a security assessment provider that could put in place a threat and vulnerability management program that could be self-managed, continuously benchmarked and enhanced. NetSPI leveraged its proven assessment methodology that focuses on seven critical areas including: asset management, configuration management, vulnerability and patch management, software development security, technical testing, threat intelligence and monitoring, as well as incident response. To ensure all critical areas were examined, NetSPI followed a phased approach spanning information gathering/planning, technology review, network security architecture review, gap analysis and documentation, external penetration testing and internal penetration testing. 2. <b>Financial Services</b> : integrating disparate processes with a cohesive strategy. By integrating and implementing these mission-critical tools and processes, NetSPI was able to create a solution that provided developers, application security engineers, and network security engineers with a seamless view of all reported vulnerabilities and supporting data. CVM ranks each vulnerability by level of risk, and data is provided to help address each instance in order of severity according to predetermined, policy driven timelines. 3. <b>Financial Services Firm</b> : complete internal penetration testing of all internal networks in four days. Beyond allowing physical access to the network, no information would be provided to NetSPI. Acting as malicious insiders that had breached the network perimeter and gained physical access to the internal network, NetSPI consultants were to emulate an Advanced Persistent Threat (APT) and report their findings.4. <b>Xcel energy nuclear</b> :examined the company's network architecture, especially its network segmentation, data flow, and security controls. One objective was to ensure the separation of business applications from plant systems, to prevent a problem with an office application from affecting the critical plant process systems and networks. corporate-level and plant-level vulnerability assessments that addressed the security of networks, servers, and applications. In a project for one plant, NetSPI performed a test to detect unauthorized wireless access points (APs). 5. <b>Security Testing for M&amp;A: Rapid Remediation supported by Resolve</b> A six-person security team set about testing two web-based applications as well as conducting external and internal penetration tests using both automated and manual processes. Because of significant time pressure, NetSPI ran all of the tests concurrently. (Not government experience. Narrow scope of penetration testing work with most projects having broader security review objectives related to process and governance. not seeing thick client, OT SCADA penetration testing just vulnerability assessment)
Staffing (30%)	30.0	15.0	1. <b>Antti, 10 years of computer security consulting experience.</b> healthcare, financial, and educational institutions. He is both a network and application penetration testing expert. He is a resource for other team members and has found numerous zero-day vulnerabilities. Highlights Recently, Antti has been focused on credentialed database hopping, exploiting the trusted relationships in untrusted environments. He has co-developed a number of NetSPI's internal tools surrounding this and other areas of penetration testing. 2. <b>Elling</b> focuses on web application and network penetration testing. He also helps with research, tool development for the assessment team, and contributes technical security blog posts. His recent research interests include dynamic binary instrumentation with the Intel Pin tool. Thomas has contributed to the Powerup SQL toolset and is the author of goddi (go dump domain info), a tool written in Go that enumerates Active Directory domain information. Certifications: 2 GIAC GPEN 3. <b>Eric</b> focusing on networking, security, and software engineering Eric's primary responsibility is maintaining and executing the thick application penetration testing service. He also has extensive experience in performing network, cloud, mobile, and web application penetration testing 4. <b>Trevor</b> r eight years of systems administration and defensive security for a state government, Trevor joined the Silent Break team in 2016 which merged with NetSPI in late 2020. He has been instrumental in developing malware, co-authoring Dark Side Ops, leading the network team in red teaming. CIAC security essentials, GIAC GCIH, GPEN 5. <b>Paroksh, practice director</b> , 8 years of experience in identifying and remediating software security vulnerabilities for a variety of organizations including financial and technology companies. Paroksh has assisted clients in building and maturing secure software development life cycle, delivering code review assessment, adopting and integrating secure code review in DevOps workflow, and performing cloud security configuration reviews. 6. <b>Ben</b> been with NetSPI since 2016 and primarily focuses on web, mobile, and network penetration tests 7. <b>Larry</b> 's primary responsibility is maintaining and executing the IOT/Embedded penetration testing service and researching new security techniques to ensure the safety of embedded systems.8. <b>Rich</b> is a Practice Director focused on Red Team Operations at NetSPI, including black box, assumed breach, and collaborative assessments security and risk assessments, security training, incident response, penetration testing, and various custom security projects as an information security consultant (not clear how much experience Elling and Eric and Trevor and Larry, have in penetration testing; Paroksh is not a penetration tester; not a deep bench of highly experienced penetration testers but IT security and some good penetration testing experience)
Qualifications Section Total Score	65.0	36.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	12.0	<b>Targets included network penetration test one week, also submitted a separate application test also about one week.</b> The content and remediation steps are clear <b>yes</b> . Separate sections for management and technical audiences; <b>yes</b>  An executive summary that presents findings, conclusions and recommendations; <b>YES. and described the scope of attacks in and out of scope</b>  Testing methodology and a description of procedures used - testing methodologies should be described at a level of detail so that they are re-creatable using screen prints as necessary; <b>Yes and in Appendix</b>  All test results and findings, including identification of tests performed that did not identify issues; <b>Yes but not tests that did not identify issues</b>  Ranked results with a standard rating scale (likelihood and significance) detailing the seriousness of each finding and remediation prioritization; <b>yes, very detailed remediation steps</b>  Detailed information about how each issue can be fixed and the level of effort to fix; <b>Yes not level of effort to fix</b> A description of the implications or impact of not fixing each of the issues noted; <b>the most critical level is labeled "entry Point" clearly stating the impact if not fixed. also in details impact is described</b>  An overall assessment based on the work performed for each agency and/or government including strengths and opportunities for improvement. <b>Yes don't see strengths</b>
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	48.0	
Evaluator Initials :			
Date:			

K689 - Security Assessment Services			
Vendor: SAC			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit. 200 hours. no additional information provided.
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	25.0	services cover a wide range of areas, including penetration tests, vulnerability scans, threat detection, intrusion detection, and security audits for client networks. Our team of highly qualified cyber security experts have decades of experience across industries and organizations, including start-ups, enterprises, and public sector institutions. CISM, CISSP, CEH, GIAC, GWAPT, GPEN, OSCP. Our team has recently accomplished a NIST Assessment and Penetration Testing project for Pierce County, which entailed an almost identical Scope of Work, comprehensive reporting, an Executive Summary & Presentation for Pierce County Leadership. Project. <b>1. Large WA County:</b> Penetration testing Internal and external for network infrastructure, cloud applications and industrial Control Systems . 2 months . <b>Project 2: Large WA County,</b> identify gaps in the cybersecurity maturity model. NIST Assessment report . 2 months, <b>Not a penetration test.</b> <b>project 3 :</b> Large CA County. Upgraded network security monitoring platform for 1000+ network devices due to SolarWinds hack. - Integrated platform with ServiceNow.- Deployed SIEM system, and NIDS & HIDS to detect intrusions and stop cyber attacks. Configured advanced features to proactively generate threshold-based alarms. Implemented Industry standard security recommendations to further improve network security. <b>not a penetration test.</b> <b>Project 4 Sheriff Department Large CA County.</b> Design, implement and test public safety first responder Sheriff's network to securely integrate their body camera and car dash camera with the Sheriff's Office network. <b>Not a penetration test.</b> <b>Project 5. : Large County Service Authority,</b> Evaluated emerging cyber threats and vulnerabilities and recommended, architected, engineered, and designed cyber-secure solution. • Planned and performed penetration testing and port scanning to identify security gaps and vulnerabilities. • Performed system log reviews to detect security breaches and policy violations. • Identified ongoing and past attacker activity in the network while improving the ability to respond effectively to future threats. • Aligned and reinforced business continuity and corporate initiatives through development and compliance management of information security policies and standards. • Deployed and managed on-premises SIEM to monitor traffic on the network for anomalies and possible compromises resulting in a 30% increased visibility of external cyber-attacks. Two more projects included in the firm experience including one with penetration test (Three of these seven projects clearly include penetration testing one has a scope similar to the project SAO intends to complete and the timeline was good. other projects include the provisioning of IT security services demonstrating great cybersecurity knowledge but not penetration testing)
Staffing (30%)	30.0	15.0	<b>1. Abhi</b> With over 21 years of intensive experience in wireless networking and security technologies, he has delivered real-world results to organizations across the country. trailblazer who has developed solutions for clients in the government, telecom, public safety, automotive, and finance industries. He will lead the SAC team and ensure exceptional service delivery to OST. <b>2. Rizwan</b> Cybersecurity Project Manager, Rizwan is responsible for governing, defining, planning, managing, and delivering products and solutions in compliance with SAC's Cybersecurity policies. He brings over 27 years of experience in cybersecurity, project management (it projects, wireless/telecom projects), and system / network administration. 3. Rob is a senior cybersecurity professional with 20+ years of in-depth hands-on cybersecurity, information security, and IT DevOps experience. <b>3. Rob</b> 20 + years is skilled in designing, developing, and implementing information security solutions, and managing security DevOps. Specializing in vulnerability and risk analysis, penetration testing, advanced persistent threat mitigation, and digital forensics and incident response. Specialties Include enterprise cybersecurity architecture, threat analysis and vulnerability assessment, red team operations and penetration testing, database and application hardening, and big data integration and encryption. <b>4. William,</b> 14 years of practical experience. He specializes in penetration testing, vulnerability management, compliance, managed security, and risk assessment. William brings evolved security solutions and testing methods to meet the challenge of continually evolving threats. <b>5. Wilder,</b> h 12+ years of exposure in the industry. Solution-focused and resourceful IT Governance Professional, offering extensive hands-on experience in implementing services centered around global information security, cybersecurity assessments, enterprise level IT risk assessment, third-party vendor risk management and tracking enterprise compliance across various security frameworks, including but not limited to PCI-DSS, ISO 27001, ISO 27002, ISO27005, HIPAA, NIST-CSF, NIST SP 800-30, SOC2, etc. (All five staff have excellent cybersecurity backgrounds. two are penetration testers and their experience with penetration testing is not clear, their years of experience with penetration testing is not clear)
Qualifications Section Total Score	65.0	40.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	12.0	<b>Targets included internal network testing.</b> The content and remediation steps are clear <b>yes.</b> Separate sections for management and technical audiences; <b>Yes</b>  An executive summary that presents findings, conclusions and recommendations; <b>Executive summary starts on page 9 with background information about what penetration testing is and definitions.</b>  Testing methodology and a description of procedures used - testing methodologies should be described at a level of detail so that they are re-creatable using screen prints as necessary; <b>clearly described the objective of the testing</b>  All test results and findings, including identification of tests performed that did not identify issues; <b>yes but not those that did not identify issues</b>  Ranked results with a standard rating scale (likelihood and significance) detailing the seriousness of each finding and remediation prioritization; <b>Yes</b>  Detailed information about how each issue can be fixed and the level of effort to fix; <b>Yes not level of effort to fix</b> A description of the implications or impact of not fixing each of the issues noted; <b>yes</b>  An overall assessment based on the work performed for each agency and/or government including strengths and opportunities for improvement. <b>Yes, overall security posture and on a positive note</b>
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	52.0	
Evaluator Initials :			
Date:			



Shorebreak			
K689 - Security Assessment Services			
Vendor: Shorebreak			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit. 835 hours is a large amount of hours. the findings from the penetration test and vulnerability assessment will be used to provide information security guidance that is fully aligned with industry standards and best practices and methodologies. Methodology included but not separate for each type of asset in the list quote. The testing schedule is good, two weeks analysis two weeks and reporting 19 days and it is clear several testing activities take place during the same time period or simultaneously.
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	32.0	Our highly credentialed security engineers provide testing and assessment services similar in scope as the SAO to both local and federal government organizations. Over 25 years of experience providing threat protection and cyber security services □ Over 30 years of combined staff experience in penetration testing□ Highly experienced and credentialed staff possessing CISSP, ECSCA, CICP, OMA, Security+, Linux+, NFA, and OSCP certifications, and more. Work for NOAA US DOE. over a decade of experience testing mission-critical systems without impacting their availability. designed to emulate real-world threats of varying degrees -from the "script kiddie" to the highly sophisticated, persistent attacker. Findings reported in real time using Lifeguard. Testing complete in a two week time frame, two more weeks for reporting. developed its network penetration testing methodology based on years of experience in network administration, penetration testing, integration engineering, and incident response. Testing procedures will include non-destructive testing techniques, including manual analysis of identified vulnerabilities and flaws. extensive experience providing vulnerability assessments that include web applications, thick client applications, mainframes, operational technology, network, and source code. f testing on the national mission critical forecast centers such as the National Tsunami Warning Center, Storm Prediction Center, National Hurricane Center, Pacific Tsunami warning Center, Space Weather Prediction Center, and others. These centers are 24/7 forecast hubs that have operational networks which require constant availability. 1. <b>1: State University Healthcare System Continuous Penetration Testing</b> . since 2014 Lifeguard scans customer networks at specified intervals using the latest vulnerability signatures looking for open ports and common vulnerabilities. Shorebreak penetration testers then validate the results from these scans to rule out any false-positive or false-negative results. These efforts are paired with manual penetration testing efforts conducted by Shorebreak's team of penetration testers. Once a vulnerability is discovered, a 'finding' is created, and the customer is notified - networks assessed every week and host discovery scans every 15 minutes. <b>2: Federal Government Regulatory Agency Penetration Test</b> , long term partner of a federal government agency. social engineering and external and internal network assessments. <b>Case Study 3: National Department of Energy Laboratory Penetration Test</b> , since 2021 numerous penetration tests every year. <b>Case Study 4: Department of Energy Research and Development Laboratory Penetration Test</b> 2021 and 2022, Shorebreak conducted manual and automated vulnerability testing against the Department of Energy lab's Information Technology (IT) assets as part of Shorebreak's Lifeguard Continuous Penetration Testing Services ("Lifeguard Services"). The focus of this testing was discovery and attempted exploitation of security flaws in the services and software running on discovered the lab's IT assets ( <b>some confidential information potentially</b> ) <b>Case Study 5: Commercial Global Satellite Communications Company</b> : network testing web application. (Excellent government experience, experience with highly mission critical systems that require continuous availability, good government experience)
Staffing (30%)	30.0	25.0	<b>1. Michael -A program manager</b> 20 years experience in information systems security will also help identify focus areas for penetration testing and plan the tests. recently led teams who verified security boundaries and validated security controls for Missile Warning Centers and a Surveillance Radar Site in Asia, and led a team who performed a security assessments for Department of Defense partner nations in the Middle East <b>2. Jose</b> A test and assessment manager will be assigned to lead the security assessment and penetration testing efforts . CISSP, ECSCA, CISP, OMA, Security +, Linux+, NFA and OSCP. Responsible for developing the ROE, daily updates and results document. Coordinate with our team of security engineers, penetration testers, infrastructure security subject matter experts, and vulnerability assessment subject matter experts to begin testing in accordance with the ROE, and complete each test within the two week time frame, 22 years of experience in the fields of system integration, installation, technical support and IT security infrastructure. As the Technical Services SME during the last 14 years Jose's main responsibilities include implementing infrastructure and network security protocols. . <b>3. Nicholas</b> test and assessment manager, ten years of experience studying offensive and defensive cyber security techniques and procedures. He served as a Technical Lead for the US Navy Red Team, performing nearly 50 assessments emulating Nation-State cyber threats. He has designed and implemented network security monitoring capabilities using open source software to monitor multiple large-scale enterprise networks centrally and efficiently. Nicholas was integral in the development of course material for a class in advanced offensive cyber methodologies primarily using PowerShell and Windows Management Instrumentation (WMI). He has also conducted incident response as well as hundreds of penetration tests, physical security assessments, social engineering campaigns, vulnerability assessments, and technical audits for Government and private sector clients alike. Certified Security Assessor (ECSCA), Certified Hacking Forensic Investigator (CHFI), Offensive Methodology and Analysis (OMA), Core IMPACT Certified Professional (CICP), Security+, Linux+, and Network Forensics Analyst (NFA)4. <b>Erik test and assessment</b> managernine years of experience in the Information Technology and Security field, and over five years of full time professional penetration testing experience OSCP and CISSP. <b>5. Brad Security</b> engineer penetration tester; 10 years of experience studying offensive security. Brad is a U.S. Army Airborne veteran with an Associate of Science (AS) in cyber security. Brad has earned his Offensive Security Certified Professional (OSCP) and network support technician certificates. 6. <b>Alberto Security engineer</b> and penetration tester, 7 years of experience in Information Security. He was lead operator for the United States Army, Cyber Protection Brigade and his duties included: adversary tactic emulation against APTs during all Incident Response engagements, rapid exploit weaponization, Red Teaming for detection engineers. He was the threat hunting lead on large scale enterprises consistent with 10K endpoints. His skills include: Red Teaming, Penetration Testing, Application Security Threat Hunting, Detection Engineering, Network Security, Infrastructure, Programming. <b>7. Hai, Security engineer</b> and penetration tester, 10 years experience in cyber security in the federal government , 8. <b>Felix. Vulnerability</b> management SME. prepared systems and applications for vulnerability and interoperability testing for 15 years. He has focused on the hardening of systems following NIST compliance process addressing security controls. Felix is well-prepared to map findings to controls and contribute best practices for vulnerability management (not clear how much experience some of the testers have with penetration testing but they all have good cybersecurity backgrounds and experience listed just not how much. the program manager and test and assessment manager have good cybersecurity background; six testers)
Qualifications Section Total Score	65.0	57.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	14.0	<b>Targets included web application, mobile application, external network, social engineering and internal network- one week</b> . The content and remediation steps are clear <b>Yes</b> . Separate sections for management and technical audiences; <b>Executive summary is technical and quite long, although very interesting for IT personnel as they walk through the specific steps that lead to discovery of vulnerabilities and how those vulnerabilities were leveraged and the impact of those vulnerabilities. Executive Summary conclusion is brief.</b>  An executive summary that presents findings, conclusions and recommendations; <b>YES</b> .  Testing methodology and a description of procedures used - testing methodologies should be described at a level of detail so that they are re-creatable using screen prints as necessary; <b>Yes</b>  All test results and findings, including identification of tests performed that did not identify issues; <b>Yes but not tests that did not identify issues</b>  Ranked results with a standard rating scale (likelihood and significance) detailing the seriousness of each finding and remediation prioritization; <b>Yes</b>  Detailed information about how each issue can be fixed and the level of effort to fix; yes but not level of effort to fix <b>Yes but not level of effort</b> A description of the implications or impact of not fixing each of the issues noted; <b>Yes</b>  An overall assessment based on the work performed for each agency and/or government including strengths and opportunities for improvement. <b>Yes, the executive summary includes positive observations and the executive summary conclusion gave an overall assessment.</b>
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	71.0	
Evaluator Initials :			
Date:			
Lifeguard provides customers with relevant findings and pertinent information IN REAL TIME without waiting on an often lengthy report process. Not only does Lifeguard allow customers to view findings quickly, but it also allows us to conduct remediation validation testing "along the way", often closing many findings before the penetration test is over. Our customer's IT staff are always in the loop, and there is no waiting for important vulnerability data is is just external networks or what is the scope of lifeguard.			

Soteria

K689 - Security Assessment Services			
Vendor: Soteria			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit. 463 hours. Testing would last three weeks. General methodology provided but not specific to the types of testing in the scope of work.
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	32.0	<b>Project 1: State of South Carolina</b> , Department of Administration: Assessment of 78 state agencies over a three year time span. Security monitoring and analytics, security incident response, and security assessment services. completed 51 state agencies including penetration testing for many state agencies. <b>Project 2: South Carolina State election Commission</b> . Penetration testing of Election voting technology including external and internal network, web application, thick client, mobile application testing and hardware. five years. <b>Project 3: Redacted</b> : annual penetration testing 2029-2022 including external and internal network, social engineering, and physical testing. <b>Project 4: Redacted</b> : red team and adversarial emulation from both an external and internal perspective attempting to gain access to the company and compromise protected assets on the internal network while avoiding detection. <b>Project 5, Redacted</b> : network penetration testing of external and internal and wireless and ICS OT vulnerability assessment. done for annual security requirements - 14 internet facing assets, internal network test on 400 in scope assets wireless on two SSOD, 75 assets in the OT environment. 2 weeks. (recent experience with the penetration testing types listed in the RFQQ, two of the projects were completed for government, first project is extensive for state government, project 5 scope is good timing given the scope)
Staffing (30%)	30.0	26.0	<b>1. Scott Thomas</b> : leads Soteria's Offensive Security team providing Red Team, Penetration Testing, and Vulnerability Management services for clients across a diverse range of industries including financial services, government, pharmaceuticals, and manufacturing. over 22 years of experience as a cybersecurity professional with a focus on offensive security operations and technologies. penetration testing experience in industrial control system environments for clients in the energy, manufacturing, chemical, and water sectors Europe, Middle East and Asia. OSCP. GICSP CISSP. <b>Mike Dame</b> : a senior cyber security specialist with expertise in Red Teaming, Network Penetration Testing, Web Application Penetration Testing, and Mobile Penetration Testing. Mike's career started in automotive IT as a penetration tester for Ford Motor Company's red team, and as a Lead member of General Motor's Red Team penetration tests on clients' critical assets and infrastructure including external penetration tests, internal penetration tests, and web application penetration tests, OSCP, eCPPTv2, CRT0, PNPT, CRTP. <b>3. Chris Slempa</b> . over 10 years experience in IT support services and field-repair for the State of South Carolina systems administrator performs 4 years penetration tests, vulnerability assessments, and provides cyber security consulting, Security +, Network + and A+. <b>4. Carl Littrell</b> , Information Security Engineer with a focus on Microsoft technologies. Carl joined oteria in 2021 as an Engineer to assist Soteria's clients with secure configuration of their Microsoft 365 environments. Carl's background in general Information Technology practices, Network Administration, and Information Security in the healthcare industry lends an in-depth understanding of the complexities in both technical and compliance requirements of business operations spanning multiple industries Network+ A+ GIAC- CGIH and GSEC. <b>5. Jevin Eskridge</b> execute and lead offensive security engagements such as vulnerability assessments, penetration tests, and red team exercises. Executes and leads full-spectrum penetration testing engagements through the entirety of project lifecycles; performs activities such as leading scoping calls, communicating with clients, conducting technical assessments, and writing commercial-grade reports. ● Executes vulnerability assessments and operates managed vulnerability scanning services; performs activities such as configuring vulnerability scans, processing vulnerability scan results, assisting with the maintenance of infrastructure relating to reporting automation. QA. develops scripts and tools to automate tasks for offensive security. Works as a security researcher disclosing security vulnerabilities. CCENT, Analyst+. eJPTv1, Pen Test+ eCPPTv2, Security+ CNSP, CVAP, CNSP. <b>6. Charles Bell 25</b> year career in IT that included infrastructure design and security for clients that spanned from Library of Congress conservationists and Fortune 100 companies to cities, school districts, and municipal governments around the country. An internationally competitive hacker, cofounder and lead co-educator for the hacking collective Strawhacks which currently has 77 members, several of which are internationally ranked. penetration testing of infrastructure. OSEP, OSCP, A+. <b>7. Brandon Halley</b> . penetration tester and security advisor, three years performs penetration testing and vulnerability assessments, Network+. Security+, Linux +, Pentest+. <b>8. Lauren Schifano</b> . DFIR examiner, not a penetration tester, Digital Forensics and Incident Response Examiner, 3 years, system administrator one year 4 years in IT. GIAC certified incident handler, CISSP, CCNA Security and CCNA, Security + . <b>9. Jonathan, AWS Security Engineer</b> , 20 years of experience in the Information Technology and Security, not a penetration tester 14 Cloud security certifications including CCSK, CCSP, and AWS Security Specialty, Security + Network+, CYSA+, CCSK, CCSP, CISSP. <b>10. Paul Ihme, co-founder and managing principal</b> currently leads the firm's detection and response efforts teams, to include the managed services, incident response, and software engineering teams eighteen years of experience in multiple information technology domains, specializing in computer network exploitation, computer network defense, and security incident response -not a penetration tester but under experience he is noted as conducting penetration testing and a strong background in cybersecurity. His career expertise includes planning, coordinating, and performing offensive computer operations for the National Security Agency, as well as defense of large, multi-layered networks at JP Morgan Chase and the Internal Revenue Service while working in their respective Security Operation Centers <b>11. Pam</b> , experienced technology strategist, project manager, and security consultant. served as CIO at the SC Ports Authority for 18 years. she held several IT management positions over 17 years at the Medical University of South Carolina in software development and healthcare systems Leads Advisory Services and Offensive Security professionals and provides vCISO services, risk assessments, security penetration tests, social engineering, and security awareness training, CISSP (Seven team members have experience in penetration testing and are penetration testers, not clear what Lauren, Jonathan or Paul's role would be perhaps just introducing; Scott and Pam are both leads - Scott has penetration testing experience Pam does not)
Qualifications Section Total Score	65.0	58.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	11.0	<b>Targets included external and internal red team assessment simulating Advanced persistent threat actors and test SOC - no scope limitation.</b> The content and remediation steps are clear <b>Yes</b> . Separate sections for management and technical audiences; <b>YES</b>  An executive summary that presents findings, conclusions and recommendations; <b>Yes. recommendations tend to address the route cause of the issues</b>  Testing methodology and a description of procedures used - testing methodologies should be described at a level of detail so that they are re-creatable using screen prints as necessary; <b>Yes</b>  All test results and findings, including identification of tests performed that did not identify issues; <b>YES and tests that did not identify issues</b>  Ranked results with a standard rating scale (likelihood and significance) detailing the seriousness of each finding and remediation prioritization; <b>NO- I see that they have severity classification on the last page of the quotations exhibit C, but I don't see it associated with the findings included in the sample report.</b>  Detailed information about how each issue can be fixed and the level of effort to fix; <b>Yes but not level of effort</b> A description of the implications or impact of not fixing each of the issues noted; <b>Yes</b>  An overall assessment based on the work performed for each agency and/or government including strengths and opportunities for improvement. <b>Yes in the executive Summary section 1.1 and 1.2; 3.2 and 4.3 outcomes clearly outline objectives and results - this shows how the organization faired in each test both positive and negative results.</b>
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	69.0	
Evaluator Initials :			
Date:			



K689 - Security Assessment Services			
Vendor: Spirent			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit. 440 hours. 55 days of testing noting but not specifying some done sequentially concurrently happening - 4-5 weeks total including testing and reporting - good timeline. Very well detailed methodology for each type of target technology included in the RFQQ sample agency.
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	32.0	Security Labs team of experts are dedicated to providing penetration testing, managed vulnerability scanning services, and security best practices training. Our team has experience working with numerous global institutions providing scanning and penetration services on networks, applications, and IoT devices as well as source code analysis with extensive experience with local government clients. Certifications OSCP (Offensive Security Certified Professional) • OSCE (Offensive Security certified Expert)• OSWE (Offensive Security Web Expert)• GXPN (GIAC Certified exploit researcher and advanced penetration tester)• GPEN (GIAC Penetration Tester)• GICSP (Global Industrial Cyber Security Professional)• NSA ISAM (NSA InfoSec assessment Methodology Certification)• CISSP (Certified Information Systems Security Professional)• CREST CCT APP (Crest Certified Tester – Applications)• CREST CPSA (CREST Practitioner Security Analyst)• CREST CRT (CREST Registered penetration Tester)• UCP (Unix Certified Programmer) (Provided a very detailed response and methodology associated with each of the types of target technologies included in the RFQQ) <b>1. City Government:</b> : Penetration Testing – External and Internal Network, Web Application, Log4J Assessment, PCI Assessment, Privacy Assessment, and Compromise Assessment, Firewall Risk Assessment, Cloud Environment Pen Test, PD Computer Aided Dispatch (CAD) Risk Assessment, PD Patrol Car and Fleet Works Risk Assessments. <b>Public Utility District:</b> Penetration Testing – External and Internal Network, Wireless Network and SCADA environment SCADA Network port scanning and service banner evaluation <b>Project 3: City Government</b> , penetration Testing – External and Internal Network, Wireless Network, Social Engineering and Compromise Assessment. <b>Project 4. US Transit Authority.</b> Red Team Engagement• Penetration testing of the payment system, electronic ticketing system, payment infrastructure, ICS/SCADA systems, DVR/camera systems, trackside systems, power delivery systems, radio systems, currently procured and future locomotives and passenger cars, business systems and business and mobile applications. • Project also includes Red Team Testing and kinetic wargaming with public transit Police. <b>Project 5: City Government:</b> Internal Network assessment, external Network assessment, SCADA assessment, Physical Security assessment (Provided a very detailed response and methodology associated with each of the types of target technologies included in the RFQQ; Project scopes closely match the RFQQ requested services ; excellent precautions noted. no mention of recently testing thick clients or mainframe specifically but it is addressed in the methodology)
Staffing (30%)	30.0	28.0	<b>1. Habib Ullah:</b> 10 years as an IT security professional <b>2 years</b> – Conduct security assessments and penetration testing of various technologies, including but not limited to web applications, web services, network infrastructures, and cloud environments. <u>plus four years-</u> Oversaw a team of 5 staff responsible for 300+ penetration projects, including banks, hospitals, and universities. Accolades in blue team and red team National cyber defense competition. Certified Information Systems Security professional (CISSP) – (ISC)2 Offensive Security Certified Professional (OSCP) – Offensive Security Offensive Security Experienced Penetration Tester (OSEP) – Offensive Security, Offensive Security Web Expert (OSWE) – Offensive Security, Cisco Certified Network Associate (CCNA) <b>2. Joshua Brown.</b> CISSP, GSEC, GXPN, GPEN, OSCP <b>2 years</b> Performing Network & Embedded Device Vulnerability Assessment, Penetration Testing and delivering results to clients. Performing Manual security assessments on network and embedded devices. Solving Network and Hardware Security problems. Assist with the developing automated tools. <b>3. Prashantkumar:</b> 11+ years' experience in application security, risk management and penetration testing, CISSP• CompTIA Pentest++ Certified Kubernetes Administrator (CKA), Certified Kubernetes Security Specialist (CKS) • AWS Certified Solutions Architect – Associate, AWS Certified Security - Specialty. <b>4. Shiv:</b> 10 years of experience in Application Security with strong knowledge in system design, integration, and management Expert in Vulnerability assessment and manual penetration testing of web & mobile applications and network systems.§ Strong technical knowledge of security engineering, computer and network security, authentication and cryptography. <b>5. Tej:</b> 5 years. <b>20 years</b> IT security <u>professional</u> Leading a team of security engineers, responsible for performing planning, assessments, analysis, detailed remediation reports for security and privacy risk assessments, security architecture reviews and source code analysis, and the execution of projects. <b>6. Tyler Bennett:</b> 2 years, Performing Network & Embedded Device Vulnerability Assessment, Penetration Testing. CompTIA A+, Network+, Security+, Project+, pen test+. (Six key staff, all have penetration testing experience and Tyler and Joshua has the least with 2 years. Not all experience clearly aligns with RFQQ requirements but some testers have deep knowledge and experience)
Qualifications Section Total Score	65.0	60.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	10.0	<b>Targets included a mobile application security assessment; network penetration test; source code scan web application.</b> The content and remediation steps are clear <b>yes</b> . Separate sections for management and technical audiences; <b>There is a one page summary that dives right into the finding without context and its technical also a results table on page two, very technical. The narrative in Network sample report was helpful in addressing this.</b>  An executive summary that presents findings, conclusions and recommendations; <b>.Yes summary of findings and conclusions No to recommendations.</b>  Testing methodology and a description of procedures used - testing methodologies should be described at a level of detail so that they are re-creatable using screen prints as necessary; <b>Yes</b>  All test results and findings, including identification of tests performed that did not identify issues; <b>Yes but not tests that did not identify issues.</b>  Ranked results with a standard rating scale (likelihood and significance) detailing the seriousness of each finding and remediation prioritization; <b>YES but there is not a definition of what the different ratings mean</b>  Detailed information about how each issue can be fixed and the level of effort to fix; <b>yes not level of effort</b> A description of the implications or impact of not fixing each of the issues noted; <b>yes</b>  An overall assessment based on the work performed for each agency and/or government including strengths and opportunities for improvement. <b>Yes in the Summary, but in the network sample report narrative it is further summarized but not the mobile application. web app report or the source code scan as they did not include a narrative - no reports included strengths</b>
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	70.0	
Evaluator Initials :			
Date:			

This is great mapping recommendations to best practices: recommendations for immediate mitigations in accordance with critical infrastructure protection recommendations, emergency management best practices, and national security special event (NSSE) requirements aligned to the NIST Cybersecurity Framework, NIST SP 800-53, NIST SP 800-82 and CIS Critical Controls for any discovered security risk, it’s significance, impact, suggested remediation

Summit			
K689 - Security Assessment Services			
Vendor: Summit			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit. 480 hours. development of proof-of-concept demonstrations and exploits for identified vulnerabilities, where appropriate. These provide analysts with a far deeper understanding of both the difficulty of exploiting specific flaws, as well as the sensitive data that may be disclosed if the issue were exploited by an adversary. This knowledge provides a stronger basis for estimating the overall risk of the issue, allowing for a better allocation of remediation resources. Summit assigns three base ratings to each finding, which are the <u>Business Impact, Relative Likelihood, and Remediation Effort</u> . 4 Engineers assigned to the testing 2 weeks for testing. This is a good timeline. General methodology described but not specific to all assets outlined in the agency sample.
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	30.0	<u>Project 1. Internal Network Vulnerability Assessment</u> . Healthcare. 2 days. <u>Project 2. Internal Network Vulnerability Assessment</u> : high level overview of the findings and recommendation while the technical findings offered detailed insights on the vulnerabilities discovered. <u>Project 3. Wireless Network Penetration Test</u> . non profit guide dog training. Test the security of an internal facing wireless network, <u>Project 4: Internal network penetration test</u> . Hague certified, non profit. Test the security of a large internal network, five weeks. Not for profit. <u>5. Internal network penetration test with SCADA Focus</u> . Food processing Factory. Test the security of a large, internal network that included a large number of SCADA factory devices. three weeks. <u>6. Thick client penetration test</u> . Private software vendor for local governments. five weeks. Testing the security of communications between the thick client, application server, and database was crucial to the test, as was evaluating the authorization model to ensure that read and write access to database tenants was properly restricted. project 7. Web Application penetration test: Housing Authority. test security of salesforce application suite. <u>8. Web Application penetration test</u> . financial services used by US Marshals and FDIC. two weeks (not government experience but experience with the type of IT assets listed in the RFQQ. Scope for each project is narrow compared to RFQQ)
Staffing (30%)	30.0	27.0	<u>1. Shawn</u> . Senior Security Consultant. CISSP, AWS Certified solutions Architect, CEH TIA A+, NET+, SEC+. Over 15 years of industry experience in information technology, privacy, and security. <u>2. Osborn</u> . Security Engineer. OSCP, eJPT. Osborn is an Information Security professional with five years of experience in the Information Technology industry. John has worked in a variety of roles, from hardware manufacturing, to system administration, to penetration testing. skilled network penetration tester with most of his experience residing in the exploitation of internal networks and Active Directory environments. He draws upon advanced red team tactics, such as payload obfuscation, credential relaying, and antivirus evasion to exploit corporate environments. On multiple occasions, John has successfully elevated his privileges from a standard user to Domain Administrator. 2 CVE publications <u>3.Porter</u> : CySA+ and ISC2, Jacob is proficient at conducting a wide variety of security assessments. He has performed hundreds of security assessments, many of which were external facing network tests that included vast OSINT research, social engineering and web application testing he has held two lead penetration tester roles at two separate firms and is now a Security Engineer at Summit. <u>4. Soltero</u> . has some healthcare, education, transit experience. CISSP over 6 years of experience in auditing information technology, privacy, regulatory compliance, and security. His expertise includes leading technical reviews of organizational controls and assessing the security posture of organizations. information security and privacy professional with experience as an Information Technology Auditor in the tribal casino gaming and hospitality industry. He has extensive experience in auditing information technology, security, data privacy, and data protection across many industries, including financial, retail, food service, higher education, software, international adoption agency, healthcare, and hospitality. <u>5. Oscar</u> . Security engineer, OSCP, OSWE, information Technology professional with over 5 years of experience in information technology, privacy, and security. During his career, Oscar has performed penetration tests and secure code reviews for multiple organizations in the private and public sector. <u>6. Hastings</u> : OWASP, an Information Technology professional with over 10 years of experience in information technology, privacy, and security. His expertise includes cybersecurity consulting, penetration testing, and red teaming. During his career, Thom has formed offensive security programs, written internal tools, publications and books, done original security research, and even dumpster dived to gather physical evidence. <u>7. Lambourne</u> : an Information Technology professional with over 20 years of industry experience in information technology, security, and software development <u>not a penetration tester</u> <u>8. Metzler</u> : Web application penetration tester certification, specializes in conducting application security assessments and cloud configuration reviews (Shawn and Lamborurn do not have penetration testing on resumes but it does note that Shawn uses penetration testing tools also don't see that Soltero is a penetration tester although he has an IT background. 2 penetration testers on with five years experience, a third with some penetest experience and 5 years in IT, a fourth with 10 years experience Limited state and local government experience, a fifth with unclear pentest experience).
Qualifications Section Total Score	65.0	57.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	13.0	<b>Targets included application security assessment and network penetration test of the xxx application and network environment.</b> The content and remediation steps are clear <b>Yes</b> . Separate sections for management and technical audiences; <b>yes</b>  An executive summary that presents findings, conclusions and recommendations; <b>Yes - the remediation categories, application development system configuration and third party software are good.</b>  Testing methodology and a description of procedures used - testing methodologies should be described at a level of detail so that they are re-creatable using screen prints as necessary; <b>Yes</b>  All test results and findings, including identification of tests performed that did not identify issues; <b>Yes not testing results that did not identify issues</b>  Ranked results with a standard rating scale (likelihood and significance) detailing the seriousness of each finding and remediation prioritization; <b>YES</b>  Detailed information about how each issue can be fixed and the level of effort to fix; <b>Yes and Yes to the level of effort to fix</b> A description of the implications or impact of not fixing each of the issues noted; <b>Yes in the remediation priorities under risk</b>  An overall assessment based on the work performed for each agency and/or government including strengths and opportunities for improvement. <b>Yes but not strengths.</b>
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	70.0	
Evaluator Initials :			
Date:			



SystemSoft			
K689 - Security Assessment Services			
Vendor: System Soft			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit. 1,900 hours seems high. no detail provided
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	21.0	over 20 years, System Soft has served as a trusted security advisor providing solutions and resources for modern security services, technologies, and expertise for reducing infrastructure risk and vulnerabilities to maintain compliance, mitigate threats and improve cyber-resilience. Our end-to-end security solutions help you confidently identify risks, defend your agency against security threats, protect sensitive information, secure the devices that connect your data, and meet regulatory requirements. Project 1. Superior Court of California. security penetration testing over their external perimeter networks and guest Wi-Fi networks to test, assess, measure, and be provided with a detailed report. Project 2. Pennsylvania Turnpike Commissions. multi-year contract with Pennsylvania Turnpike Commission to provide Security Assessment services. We were recently awarded a work order to perform Information Security Risk Assessments for Pennsylvania Turnpike Commissions' core Enterprise applications and infrastructure NIST Cyber Security Framework. The services will commence in December 2022 (second project is not penetration testing) Project 3: North Carolina Department of Health and Human Services. worked with the North Carolina Department of Health and Human Services (SAO) to perform a privacy and security assessment of the NC-FAST application for MARS-E, NIST 800 rev4, and HIPAA controls, federal, state, and SAO security policies and procedures. With System Soft's previous experience and understanding of MARS-E V2 and other state security policies. In addition to advanced IT certifications, System Soft conducted infrastructure penetration (PEN) testing and security testing of web applications and used its custom, proprietary security tools (developed in Python) to find various web vulnerabilities Project 4. North Carolina Department of Revenue. In the past 3 years, we have successfully completed three Cybersecurity risk assessments for NCDOR. The assessments are independent audits of NCDOR-IRS 1075 Controls and NIST 800-53 Controls. NCDOR renewed our working agreement to provide similar services for another 3 years. Administering mainframe testing. Project 5 Fayetteville Technical Community College. performed IT Security Assessments for NIST 800-53 Rev 4 moderate controls review, operating system security assessment, external and internal penetration testing, wireless network penetration testing, and web application and website security assessment (excellent state government experience, it is not clear that the second project included penetration testing and if so the scope of work is not clear. The fourth project is a penetration test. fifth project has a scope of work more similar to the work requested in the RFQQ and what our audits would typically include)
Staffing (30%)	30.0	20.0	<b>1. Mark: Vice President Enterprise Architecture.</b> Risk and Security Champion with more than 24 years of experience. Focused on various Security Assessments and Compliance Security Architecture, Enterprise Architect, Security Assessments, Cloud Strategist, Over the last 15+ years as an practitioner, Advisor, or implementor have helped many companies develop and run ARB (Architecture Review Boards) as well oversee the running or improving of ITSM/ITOM environments by designing/implementing emerging technologies like AIOps like Netcool, Moogsoft, and many other tools to improve RCA, MTTL, and MTTR. s led health insurance, financial services and public sector institutions in the design and implementation of their information security control testing, data protection, privacy, business continuity, IT Governance, Risk and Compliance (GRC) and Third-Party Risk Assessment programs. <b>2. John Nyaza Risk Assessment Specialist</b> CISSP, CEHMITRE ATT&CK Defender; Over 20 years of experience delivering enterprise IT security strategies to expand capabilities, reduce global risk exposure, and identify vulnerabilities. Leads cross-functional teams to develop and modernize IT security platforms and drive enterprise security. Proven experience leading global technology with specialized expertise in FinTech, Cybersecurity, and Big Data solutions, experience with vulnerability and penetration testing. <b>3. Craig.</b> CEH, More than 10 years' experience in Information Technology, with strong expertise in team leadership, security management and enterprise architecture. Demonstrated expertise in establishing and implementing large information security programs. Designed and implemented automated tool-based vulnerability management framework that continuously monitors, detects, and remediates Cybersecurity threats and Vulnerabilities. Performed evaluations and selections of IT enterprise and IT security tools and successfully implemented systems to protect the availability, integrity, and confidentiality of critical business information. Competencies include red teaming, Blue Team. <b>4. Cameron: Risk Assessment Specialist,</b> no penetration testing certifications, General knowledge in penetration testing and vulnerability scanning <b>5. Phani</b> ,no penetration testing certs 14 year experience in Cyber Security and Assessment. General knowledge in penetration testing and vulnerability scanning <b>6. Praneetha</b> , CISSP, CEH, Security + , 9 years of experience in Cyber Security Implementation and Assessments OWASP, Perform application penetration testing (Blackbox/Greybox /Whitebox testing) Expertise in Application Security and identifying and fixing OWASP Top 10 and SANS 25 security vulnerabilities Proficient in performing automated as well as manual vulnerability assessments and penetration testing on Web Applications and Networks. Maintain current working knowledge of web application security issues. Created and maintained various scripts for penetration testing (Mark is an IT security practitioner but I do not see that he has experience as a penetration tester, John is an IT security profession but has some penetration testing experience but it is not clear how much. Craig, the extent of his penetration testing, blue and red teaming is not clear, he has extensive IT security experience. Cameron has general knowledge of penetration testing but his experience is not clear.Phani, not clear how much penetration testing experience he has; Prameetha appears to be a proficient penetration tester)
Qualifications Section Total Score	65.0	41.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	6.0	<b>Targets included was not clear.</b> The content and remediation steps are clear <b>Yes.</b> Separate sections for management and technical audiences; <b>No</b>  An executive summary that presents findings, conclusions and recommendations; <b>No</b>  Testing methodology and a description of procedures used - testing methodologies should be described at a level of detail so that they are re-creatable using screen prints as necessary; <b>No</b>  All test results and findings, including identification of tests performed that did not identify issues; <b>Yes but not tests that did not identify issues</b>  Ranked results with a standard rating scale (likelihood and significance) detailing the seriousness of each finding and remediation prioritization; <b>Yes</b>  Detailed information about how each issue can be fixed and the level of effort to fix; <b>yes but not level of effort</b> A description of the implications or impact of not fixing each of the issues noted; <b>Yes</b>  An overall assessment based on the work performed for each agency and/or government including strengths and opportunities for improvement. <b>No</b>
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	47.0	
Evaluator Initials :			
Date:			

K689 - Security Assessment Services			
Vendor: Tevora			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit. 290 hours. Listed several requirements for testing on page 5, we would need to get a better understanding because most of our state and local governments will not have these items. Note extra charges for off hour testing, this does happen on our audits. A detailed work plan for Internal and external network testing and mobile and web applications included but not the thick client and the industrial control systems. In the cost breakdown it is not clear that all of the scope of work in the sample agency is included because the SCADA and thick client are not listed
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	30.0	over 20 years of experience in providing a wide range of services, including Penetration Testing, Enterprise Risk Assessments/Audits, Business Continuity and Disaster Recovery Plans, and Privacy Assessments. wide range of certifications and qualifications, including certifications from Global Information Assurance Certification (GIAC), Offensive Security Certified Professional (OSCP), Certified Ethical Hacker (CEH). Our experience in performing vulnerability assessments includes web applications, thick client applications, mainframes, operational technology, network, and source code. We have conducted similar assessments for SAOs in both the government and private industries and have successfully identified vulnerabilities and provided recommendations for remediation. Our team has conducted both non-invasive/passive testing in production environments containing highly sensitive information and mission-critical systems requiring high availability, as well as exploiting discovered vulnerabilities in test environments. <u>penetration testing execution standard. Project 1 – County Government in California (2023):</u> Tevora provided the following services to the client:• PCI DSS Training• PCI 4.0 Readiness Assessment• Internal and External PCI Penetration Tests• Wireless Penetration Test• PCI Network Segmentation Test (2nd Test – CUPPS Only)• Level One PCI Assessment (CUPPS)• PCI SAQ Assistance (PARCS)• Optional Ongoing Remote QSA Remediation Assistance• Monthly Vulnerability Scanning. <u>Project 2 – City Government in California (2021):</u> The city required professional services to identify ITS vulnerabilities within their systems. Tevora was tasked with performing penetration testing and advanced console audits of the computers managed by the city to produce biannual ITS reports and to identify cybersecurity breaches. Tevora was responsible for completing tasks outlined in Activity 1 for the biannual ITS report, including tasks such as external and internal penetration testing, web application penetration testing, and wireless LAN penetration testing. The activities included up to 400 network devices being considered in scope for this external pen test. The project focused on nine applications and utilized a combination of tools, utilities, and methodologies to review potential points of security failure. <u>Project 3 – Not-for-profit Cooperative Power Supplier in Colorado (2022):</u> Tevora provided internal and external penetration testing services, internal network. evaluated the impact of exploitation, tested the client's internal defenses, and used initial exploits to escalate access to additional targets. <u>Project 4 – Major Corporation who specialize in Advanced Analytics for Process Manufacturing Data</u> located in Washington (2023) Cloud Infrastructure Penetration Testing and Web Application Penetration Testing services to the client, cloud infrastructure penetration testing approach consisted of conducting an open box penetration test against the Client's cloud infrastructure to test the security of deployed resources, including computer instances and cloud native services. and the project activities involved cloud service reconnaissance, managed code and configuration review, network reconnaissance, known vulnerability identification, exploitation, and post-exploitation and assumed compromise simulation. <u>Project 5 – Best-In-Class Gaming Retailer located in Washington (2022)</u> e Longarm Kiosk Testing project phase focused on remote testing of a Nvidia-based in-store kiosk platform network communications. used a combination of tools, utilities, and methodologies to review the various potential points of security failure and attempted to exploit known weaknesses in the various security technologies to gain access to the device and device communications. Two device system platforms were considered in scope for testing, including the Longarm Kiosk. Phase 2 of the project focused on conducting a web application penetration test to identify vulnerabilities that could lead to unauthorized access of the application or the supporting environments. Tevora used a combination of tools, utilities, and methodologies to review the various potential points of security failure. The scope of the testing included the Longarm web application and Longarm APIs. Testing objectives included testing of the mobile experience with interacting with the Kiosk, persistence and security of the client's session information across all mobile use cases, and security of data flow and application logic within the web applications directly used by mobile users and any third-party connections. (Projects listed are all penetration testing with some scoped similar to the work in the RFQQ. Two of the five projects are with state government, no thick clients )
Staffing (30%)	30.0	13.0	<u>1. Sabrina Failer Roman, Director of Consulting Operations (Project Management)</u> manage the Project Management Office and Quality Assurance teams, as well as work closely with Tevora's President on strategic Operations initiatives, 20 Years experience in project management including Olympics. <u>2. Clayton Riness, Principal Consultant (Threat Services), role is practice lead PCI QSA, and the Certified Information Systems Security Professional (CISSP)</u> lead Tevora's technical practice delivery spanning Solutions, Threat, Incident Response and Cloud Security. His professional background includes 20 years of information technology and security experience spanning many technologies under the most demanding compliance and uptime requirements. n a decade of experience in IT and security, Clayton delivers/provides clients with extensive knowledge in business and technology His experience in policy reviews, security assessments, security remediation, infrastructure management, and regulatory compliance. Ensures IT engagement and secures key IT, compliance, and business resources• Provides direction related to key project decisions, addresses escalated issues• Sign-off on deliverables for all activities• Review testing results• Validate project communications. <u>3. Kevin, Technical resource:</u> Offensive Security Certified Professional (OSCP), a Splunk Certified Architect, a Certified Information Systems Security Professional (CISSP), and an ISO 27001:2013 lead auditor threat research expertise includes network, web, and mobile application penetration testing, development of internal Tevora penetration testing and social engineering toolkits, malware analysis, and incident response. Kevin also develops and administers Tevora's secure coding curriculum and training sessions. Kevin is an information security professional with expertise in penetration testing, development of security intelligence solutions, web development, mobile app development, risk management, and ISO 27001, HIPAA, and PCI assessments. (One Project manager, a Practice lead and one penetration tester, in the introduction it notes, highly skilled and experienced engineers are certified and experienced in penetration testing, possessing qualifications such as Global Information Assurance Certification (GIAC) certifications including GPEN Penetration Tester Certification, Web application Penetration Tester (GWAPT), Offensive Security Certified Professional (OSCP), Certified Ethical Hacker (CEH), and other equivalent certifications- but only one penetration tester is noted in the response- note the sample report lists 12 participants that I would assume are testers, maybe some of them are from the client being tested.)
Qualifications Section Total Score	65.0	43.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	10.0	Targets included Internal, External, & Web Application Pentest Report, 30 days of testing. The content and remediation steps are clear Yes. Separate sections for management and technical audiences; Yes but quite technical  An executive summary that presents findings, conclusions and recommendations; Yes but no to recommendations - the table of contents indicates there are strategic recommendations but when clicked it goes to the end of Web App test results, perhaps it was taken out.  Testing methodology and a description of procedures used - testing methodologies should be described at a level of detail so that they are re-creatable using screen prints as necessary; Yes and really good summary of how the attack progressed and weaknesses used to escalate and continue attack  All test results and findings, including identification of tests performed that did not identify issues; Yes but not those that did not identify findings  Ranked results with a standard rating scale (likelihood and significance) detailing the seriousness of each finding and remediation prioritization; YES- CVSS base score and hyrarisk  Detailed information about how each issue can be fixed and the level of effort to fix; Yes but not the level of effort to fix A description of the implications or impact of not fixing each of the issues noted; Yes  An overall assessment based on the work performed for each agency and/or government including strengths and opportunities for improvement. Yes, in the findings overview but not strengths.
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree its mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	53.0	
Evaluator Initials :			
Date:			

Many entities and state agencies do not have all these items Client will provide adequate access to systems and personnel as required to perform the project objectives. This includes all network diagrams, documentation, policies, systems, network access, support staff, administrative staff, and executive staff needed to complete the objectives of this Work Plan. Tevora cannot be held responsible for analysis of applications, systems, and networks to which Tevora has not been given access to (page 5) The client will provide the necessary workspace and equipment to conduct onsite work, including (but not limited to) desk space, telephone, printer access, Project Management Tools access, and conference room access as needed. Testing outside of Tevora's standard business hours is subject to a 10% surcharge. After Hours Testing: No• Testing outside of Monday-Friday is subject to a 25% surcharge. Weekend Testing: No



K689 - Security Assessment Services			
Vendor: WWT			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit. 465 hours, very high overview of general testing methodology provided- referencing methodology in the later submission.
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	14.0	Palo Alto Networks Unit 42 brings together world-renowned threat researchers, elite incident responders, and expert security consultants to create an intelligence-driven, response-ready organization that's passionate about helping you proactively manage cyber risk. Our team serves as your trusted advisor to help assess and test your security controls against the right threats, transform your security strategy with a threat-informed approach, and respond to incidents in record time so that you get back to business faster. We have provided our offensive security assessments such as pen testing to hundreds of customers. We have done this with Fortune 200 companies, small businesses, and many public sector organizations. <b>Example 1</b> school district to conduct penetration testing (both internal and external). The Unit 42 team first reviewed recent threat intelligence gathered by Unit 42 and lessons learned performing 1000s of IR investigations to determine the most common TTPs used by adversaries. We also leveraged the tool xPanse (attack surface telemetry) to determine the client's attack surface vulnerabilities that we should prioritize while testing. Our penetration testing activities then were conducted against key assets in the organization <b>Project 1. Software and Services provider:</b> Providing incident response services; investigated the attack, contained the breach, removed malware from environment, restored cloud environment and provided root cause and findings. <b>Project 2: Large financial services management company.</b> Managing funds on cryptocurrency exchanges. The company needed immediate incident response services help to identify the source of the attack, secure the environment, and provide an after-action report to help the company understand what had transpired. The organization's CISO also needed guidance on properly addressing board members' concerns about the incident and its resolution. Unit 42 incident response experts identified how and where the breach occurred, guided the client to put the proper security controls in place, and provided post-event guidance to help the CISO effectively communicate what had happened and remedies put into place to ensure it doesn't happen again. <b>Project 3 Large multinational organization.</b> Security program design and purple team exercises. Assessed client's policies and processes using NIST CSF framework + Simulated security events to test and measure security operations center team communications, capabilities, and tools. Using the Cybersecurity Framework (CSF) from the National Institute of Science and Technology (NIST) and other proprietary controls, Unit 42 assessed the client's capabilities in threat intelligence, threat hunting, threat detection, and threat response, as well as its security monitoring and reporting controls. This exercise revealed gaps in essential security operations controls, especially in the areas of threat hunting, detection, and response. ran a purple team attack simulation in the client's environment to evaluate how the security team would react to a threat in real time. The simulation involved detecting, analyzing, and resolving a security ticket. It helped Unit 42 determine the effectiveness of the client's response and communications between its Security and IT teams. <b>Project 4 Healthcare recover from ransomware.</b> Manage malware attack response, communicate with customers, lawyers, and regulators+ Build a cybersecurity strategy and reduce cyber risks moving forward. manage the breach response, manage communications, and coordinate with internal teams to create a cybersecurity strategy to answer questions about the company's security posture. <b>Project 5: Rebuilding a healthcare providers environment after a ransomware attack.</b> investigated and identified Black Cat ransomware + Helped client negotiate ransom, coordinated communications, and restored the environment Results + Client regained access to its environment + Threat actor backdoors were removed + A new approach to security made the client's system more resilient to attack. (These project require a deep knowledge of IT security and deep technical knowledge however they are not penetration testing they are incident response and recovery, some penetration testing on project three)
Staffing (30%)	30.0	15.0	<b>1. Bill.</b> GIAC Cloud Penetration Tester 2022,OSCP 2014, CISSP #351328 2009, GIAC Certified Incident Handler 2007, GIAC Security Essentials Certification 2007, Yearly FERPA/HIPAA certification since 2006, GIAC Certified Windows Security Administrator, <u>penetration tester for Palo Alto Networks 2022 to current</u> , seven year Rapid7 senior penetration tester, three years with Computer sciences corporation pen testing; six year with Purdue University, Perform security risk assessments, security consultation, penetration, testing, web application scanning, vulnerability scanning, ● Primary enterprise firewall administrator, Cisco Security Manager project lead● Forensic investigation of PCI, HIPAA, incidents● PCI compliance and PCI network re-architecture, Five years Infrastructure technologist- total at least 16 years penetration testing experience; <b>2. Walter.</b> Lead penetration testing one year, up to four teams at a time; GIAC: Cloud Penetration Tester (GCPN) Aug 2021, Offensive Security: Offensive Security Certified Professional (OSCP) Feb 2021GIAC: Certified Forensic Analyst (GCFA); Extensive knowledge of offensive security methodologies with a focus on Windows security, EDR/Antivirus, bypass techniques, and development of red team infrastructure. lead for several penetration testing engagements at a time and strategically divide testing to create a plan of attack for up to four consultants at a time, IT Security background six years. (Two personnel both with penetrating testing experience, one with 16 years at least the second has testing experience and is a team lead for numerous engagements with six year in IT security; it is not clear who else would staff these team)
Qualifications Section Total Score	65.0	29.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	9.0	<b>Targets included externally facing assets, network and web application, in order to identify potential security vulnerabilities, 18 days.</b> The content and remediation steps are clear . Separate sections for management and technical audiences;  An executive summary that presents findings, conclusions and recommendations; <b>Yes .Also included vulnerabilities sorted into categories based on the they of risk posed the organization, Information disclosure, outdated software security absence and phishing</b>  Testing methodology and a description of procedures used - testing methodologies should be described at a level of detail so that they are re-creatable using screen prints as necessary; <b>Yes</b>  All test results and findings, including identification of tests performed that did not identify issues; <b>Yes not to tests performed that did not identify issues</b>  Ranked results with a standard rating scale (likelihood and significance) detailing the seriousness of each finding and remediation prioritization; <b>Yes and for each finding gave impact of the finding and exploitability</b>  Detailed information about how each issue can be fixed and the level of effort to fix; <b>Yes no to level of effort</b> A description of the implications or impact of not fixing each of the issues noted; <b>Yes</b>  An overall assessment based on the work performed for each agency and/or government including strengths and opportunities for improvement. <b>basic in the executive summary No strengths</b>
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	38.0	
Evaluator Initials :			
Date:			